

# الجرائم المعلوماتية على شبكة الإنترنت

Internet Crime  
**Complaint  
Center**



الأستاذ

**أمير فرج يوسف**

المحامى لدى محكمة النقض  
والإدارية والدستورية العليا

2008

To file an  
complaint

# **الجرائم المعلوماتية**

## **علي شبكة الإنترنت**

## **Internet Crime**

**الأستاذ**

**أمير فرج يوسف**

المحامى لدى محكمة النقض

والإدارية والدستورية العليا

٢٠٠٨



## مقدمة

لا شك أن الجرائم المعلوماتية جرائم ولدت نتيجة لإساءة استخدام شبكة الإنترنت العنكبوتية التي ظهرت أخيراً على الساحة الدولية حيث لم يكن لها وجود قبل ذلك ونتيجة لظهور تلك الشبكة فقد ظهرت معها الجرائم المعلوماتية التي تمثلت في جرائم الاعتداء على الكمبيوتر سواء كان هذا الاعتداء يقع على ذات جهاز الكمبيوتر أو كان على البيانات المعلوماتية التي توجد على هذا الجهاز أو على الشبكة ذاتها.

والملاحظ أن هذه الجرائم الإلكترونية ما كانت أبداً في الحسبان إذ أن التاريخ البشري لم يمر قط قبل ذلك بمثل تلك التجربة الأمر الذي جعل البعض يطلق على هذا العصر عصر ثورة المعلومات باعتبارها الثورة التي تلت الثورة الصناعية.

مما لا شك فيه أن الثورة الصناعية في بدايتها كانت غريبة على العقل البشري ولكن بالتدريج استطاع الإنسان أن يستوعب تلك الآلة وينشئ المصانع والآلات التي ذهبت إلى الكواكب الأخرى ويضع القوانين التي تنظم العمل بتلك الآلات.

والحقيقة أن الثورة المعلوماتية الوليدة لا تزال في إرهاصاتها الأولى والجميع الآن يمرون بلحظة الإنبهار ومحاولة استيعاب فوائد تلك الثورة الهائلة التي اعتمدت على شبكة الإنترنت العملاقة والعنكبوتية التي تمتد وتخترق كل مكان في كوكب الأرض لا يمنعها أي حواجز سواء كانت طبيعية أو سياسية.

وترتب على ذلك أن أصبح العالم قرية صغيرة متناهية الصغر يستطيع كل فرد في هذا العالم أياً كانت الدول التي ينتمي إليها أن يتحدث ويعلم وينقل



الأفكار والأخبار وبيع ويشترى في ظل التجارة الإلكترونية التي ولدت مع بزوغ تلك الشبكة العملاقة للإنترنت.

وإذا كانت شبكة الإنترنت قد وصلت الأمم والشعوب بعضها بعض ونقلت الثقافات والخبرات ونقلت الحدث في حينه بالصوت والصورة واخترعت البريد الإلكتروني الذي من خلاله يستطيع الفرد أن يتلقى عن طريق هذا البريد كافة الرسائل والخطابات بالكتابة وبالصوت والصورة، وإذا كانت أيضاً تلك الشبكة استطاعت أن تخترق الحدود السياسية للدول النامية والمتخلفة وتكشف تلك الدول أمام شعوبها وإذا كانت تلك الشبكة الإلكترونية العملاقة المسماة بالإنترنت قد استطاعت تقديم خدمات جليلة للأمم والشعوب. إلا أن تلك العظمة الكبيرة في الفوائد والعطايا التي تقدمها تلك الشبكة كان في مقابلها من المساوئ الكثير إذ ظهرت جرائم ما كانت أبداً في الحسبان ارتبط بعض هذه الجرائم بتلك الشبكة أي جرائم واقعة علي شبكة الإنترنت ذاتها الهدف منها شلها وتعطيلها.

كانت هناك جرائم تقع علي أجهزة الكمبيوتر التي تقوم باستقبال وتشغيل شبكة الإنترنت.

ولم يقف الأمر عند هذا الحد بل ظهرت جرائم يستخدم فيها الكمبيوتر والمعلومات التي تتداول عليه من أجل الإساءة إلي الآخرين في صورة جرائم تقع علي الأشخاص ذاتهم مستخدمين تلك الأجهزة مثل الجرائم الماسة بالشرف والاعتبار والسمعة.

ناهيك عن الجرائم المعلوماتية التي هدفها تدمير وتعديل البيانات واختراق تلك النظم بهدف تزوير البيانات والمعلومات للإضرار بالغير.

ولم يقتصر الأمر علي هذا بل ظهرت علي السطح مواقع مشبوهة تهاجم الأفراد والدول والحكومات والسياسات والمعتقدات الدينية والقيم والعادات الاجتماعية.

ومما زاد الأمر تعقيدا استغلال البعض لتلك الشبكة في إدارة الأعمال المنافية للأداب والدعارة والاتجار بالصور والأفلام الجنسية وبالنساء والأطفال عبر تلك الشبكة.

ولم يقتصر الأمر علي ذلك بل زاد علي ذلك ظهور جرائم لم تكن واردة من قبل مثل جرائم تبيض وغسل الأموال والإرهاب والجريمة المنظمة بكل صورها السابقة وصورها الأخرى مثل تجارة تهريب المهاجرين والاتجار في المخدرات والمؤثرات العقلية والاتجار بالأشخاص والأطفال.

ولما كانت شبكة الإنترنت قد أظهرت لنا طوائف كثيرة من الجرائم يتعذر بحثها كلها لذلك سوف يقتصر هذا البحث علي الجرائم المعلوماتية الإلكترونية التي يقرؤها بعض المجرمين بهدف تدمير البيانات وتعديلها ومحوها ومهاجمة تلك البيانات من أجل تزويرها علي نحو يخالف الحقيقة والواقع.

ومن الجدير بالذكر أنني قد استعنت في هذا البحث بالكثير من الأبحاث من علي شبكة الإنترنت في محاولة لإظهار فكرة الجرائم المعلوماتية وختمت هذا الكتاب بالعديد من الاتفاقيات الدولية المتعلقة بشأن جرائم الكمبيوتر المعلوماتية.

ولي أمل أن يحظي هذا الجهد المتواضع بالقبول والرضا.

والله خير المستعان

أمير فرج يوسف

المحامي لدى محكمة النقض



# **فصل تمهيدي**

## **في الجرائم المعلوماتية**

## آداب السلوك الأساسية علي إنترنت:<sup>(1)</sup>

في ما يخص كلا من الطرق المختلفة المستخدمة للقاء الناس عبر إنترنت- مثل غرف المحادثة وسجلات ويب و "المساحات" الشخصية والمنديات، إضافة إلي البريد الإلكتروني والمراسلات النصية- تتوفر مدونات سلوك خطية وغير خطية.

في ما يلي بعض التلميحات العامة التي يمكنها أن تساعدك علي الشروع في العمل علي إنترنت، مع حد أدنى من العقبات وسوء التفاهم.

### المحادثات والمنديات والمجتمعات عبر إنترنت:

- إقرأ القواعد أو الإرشادات الخاصة بغرفة المحادثة أو المنتدى أو المجتمع عبر إنترنت قبل التعامل.
- حماية الخصوصية: لا تستخدم أبدا اسمك الكامل. لا تطلب الأسماء الكاملة للآخرين.
- لا تستخدم تعابير غير مناسبة.
- تجنب استخدام الأحرف الاستهلاكية الكبيرة للتأكيد فقد يفهم ذلك علي أنه "صراخ".
- فلنكن الرسائل قصيرة.
- تحقق من طريقة الكتابة الإملائية.
- في المنديات، قبل أن تبدأ بسلسلة رسائل بموضوع جديد، تحقق دوما من عدم وجود سلسلة رسائل سابقة حول الموضوع نفسه. إذا كانت تلك هي الحال، فقم بالإجابة علي تلك الرسائل السابقة.

<sup>(1)</sup> <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.msp>

## بريد إلكتروني: (١)

- لا ترسل البريد الإلكتروني غير الهام أو تعيد توجيهه.
- لا ترسل أو تعيد توجيه "خدع إنترنت" لمعرفة ما إذا كانت قصة ما حقيقية. راجع مصدرا موثوقا مثل Snopes. Com.
- لا ترسل التحذيرات من الفيروسات أو تعيد توجيهها. فقد تكون تلك خدعا.
- إذا كنت ترد علي بريد إلكتروني أصلا إلي العديد من المستلمين، فقم بالرد فقط علي الأشخاص المعنيين.
- تجنب إرسال مرفقات كبيرة إلي مستلمين متعددين.
- بشكل عام، من الجيد تذكر أنه يتم عادة فقدان الفوارق التمييزية عبر إنترنت، لتجنب سوء التفاهم، تحدث بوضوح، وكن أكثر حذرا عند المزاج مما تكون عليه عادة خارج إنترنت.
- إن الطبيعة غير الشخصية لعالم إنترنت تسهل التواصل بطريقة تتسم بالقوة أكثر مقارنة مع التواصل الشخصي من المستحسن دوماً نتساءل قل أن ترسل تعليقاتك عما إذا كنت تطلقها إذا كنت وجها لوجه مع شخص ما، في حال لم تكن لتطلقها في وجهه فقد يكون من المفيد إعادة النظر في ألفاظك.
- وفي النهاية، تذكر أن كل شيء يبقى علي ويب لمدة طويلة. من المستحسن أخذ القراء بعين الاعتبار، وقد يشمل ذلك أصحاب عمل محتملين مستقبليين بعد مرور عشر سنوات.
- إذا كنت مهتماً بمعرفة المزيد حول آداب السلوك علي إنترنت، فتستطيع محاولة البحث عن "آداب التصرف" علي ويب.

(١) <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.msp>



تشمل معظم الموسوعات علي ويب إدخالاً حول الموضوع، مع نصائح حول مسائل مثل كيفية تجنب "حروب النيران"، وهي عبارة عن ظهور مفاجئ لتبادل عدائي يطلقه أحياناً "المسوخ" (معروفين بالإنكليزية بـ trolls) وهم مستخدمون يثيرون عن قصد غضب مستخدمين آخرين، أو يقتلون النزاعات.

#### كيفية التسوق عبر إنترنت بأمان أكبر:

في حالة لم تكن تعرف شركة بيع بالتجزئة عبر إنترنت من خلال علامتها التجارية أو سمعتها، إطلع علي هذه التلميحات التي ستساعدك علي تحديد ما إذا كانت تشغل موقعاً آمناً وموثوقاً، وذلك قبل أن تدخل رقم بطاقة الائتمان الخاصة بك أو معلوماتك الشخصية.

- **تحقق من الخلفية،** ابحث عن عنوان فعلي (وليس عن صندوق البريد)، أو اطلب كاتالوج عبر البريد الإلكتروني، أو اتصل بمندوب شركة وتحدث إليه.

- **استكشف موقع ويب** بحثاً عن أختام موافقة تقدمها جهات خارجية

علي غرار:

Better Business Bureau Online) BBBOnline

أو

TRUSTe

تستطيع الشركات وضع هذه الأختام علي مواقعها إذا كانت تلتزم بمجموعة من المعايير الصارمة، مثل الطريقة التي يتم من خلالها حل الشكاوي والخلافات، وطريقة استخدام المعلومات الشخصية. إذا لم تري هذه الأختام علي الموقع بسهولة، فراجع نهج الخصوصية أو "الأحكام والشروط" التي يجب أن تكون منشورة بوضوح علي الموقع.

تلميح: إذا رأيت الأختام المذكورة أعلاه، فانقر فوقها للتأكد من أنها ترتبط بالمؤسسة التي أنشأتها. وسيقوم بعض التجار العديمي الضمير بوضع هذه الشعارات علي مواقعهم من دون إذن، وهناك احتمال بسيط بأن يتم القبض عليهم إذا لم ترتبط هذه الأختام بالموقع.

- اعرف ما يقوله المتسوقون الآخرون حول متجر عبر إنترنت علي مواقع المقارنة مثل Epinions أو Bizrate تحتوي هذه المواقع علي تقييمات العملاء المضمنة في تصاميمها مع عدد من الوجوه المبتسمة أو النجوم.

- راجع طرق الشحن والنهج لتحديد شركات النقل التي يستخدمونها، وأسعار الشحن، وما إذا كنت توفر خدمة التعقب والتأمين. كذلك استفسر عن المكان من حيث يتم الشحن، ففي بعض الأحيان يتم إرسال البضائع من مواقع عالمية، مما يتطلب دفع رسوم جمركية ويحتاج إلي وقت إضافي.

#### قبول إدخال رقم بطاقة الائتمان: (١)

لقد عثرت علي السلعة المثالية بالسعر المثالي وأصبحت جاهزا للشراء قبل إدخال رقم بطاقة الائتمان. تؤكد من التزام المتجر الذي اخترته بالقواعد التالية:

- علي الشركة أن تطلب فقط المعلومات الشخصية الضرورية لإتمام عملية الشراء، سنقوم علي الأرجح بإدخال رقم بطاقة الائتمان الخاصة بك، وعنوانك، ورقم هاتفك. يجب أن تتوخي الحذر إذا ما تمت مطالبتك بتوفير معلومات أخرى، مثل رقم التأمين الاجتماعي، أو رقم حسابك المصرفي، أو اسم عائلة أمك.

ملاحظة: قد تسألك بعض الشركات المحترمة عن اهتماماتك، فتطلب منك تحديد بعض خانات الاختيار، لا يجب أن تكون هذه المعلومات ضرورية لإتمام عملية الشراء.

(١) [http://www.microsoft.com/middleeast/arabic/athome/security/online\\_netiquette.msp](http://www.microsoft.com/middleeast/arabic/athome/security/online_netiquette.msp)

- يجب أن يستخدم الموقع علي ويب تقنية أمنة. عندما تصل إلي الشاشة حيث عليك إدخال رقم بطاقة الائتمان أو معلومات شخصية أخرى. تأكد من أن عنوان ويب يبدأ بـ http (مثلا، <https://www.tailspintoys.com>) وتحقق من ظهور قفل صغير مغلق في أسفل يمين الشاشة.

في حال أنك تستخدم Internet Explorer فستحصل علي طبقة حماية أخرى مع المواقع التي تستخدم شهادات التحقق من الصحة الموسعة (EV) SSL. يجب أن يصبح لون شريط العنوان أخضر لإعلامك بوجود المزيد من المعلومات المتوفرة حول موقع ويب. تظهر أيضا هوية مالك موقع ويب علي شريط العنوان.

إن شهادة EV SSL لا تساعد فقط علي ضمان أمان الاتصال بموقع ويب، بل تضم معلومات حول مالك موقع ويب الذي تم تحديده من قبل المرجع المصدق الذي يصدر شهادة SSL.

#### تحديد مستعرض ويب:

يشمل Internet Explorer 7 ميزات أمان إضافية تسهل عرض المواقع التي توفر تبادل البيانات الأكثر أمانا. فتستطيع التسوق وإجراء المعاملات المصرفية عبر إنترنت بثقة. لمعرفة المزيد، راجع Internet Explorer 7 ساهم في توفير حماية ضد سرقة الهوية وغيرها، قم بزيارة موقع Internet Explorer علي ويب لتتزيل المستعرض وتثبيته الآن.

#### ثق بحدسك:

إذا تطابق أحد المواقع مع كافة المعايير المذكورة أعلاه، فهناك احتمال كبير بأن يكون الموقع شرعيا وموثوقا ولكن، وكما هو الحال في معظم الأمور عبر إنترنت أو خارجها، إذا لم تكن مرتاحا تجاه متجر ما فاصرف النظر عنه وتسوق في مكان آخر.

الأصل التاريخي لجرائم الكمبيوتر وأهم وأخطر الجرائم التي ارتكبت في عصر الحوسبة وثورة المعلومات فائقة السرعة.

#### أولاً: فيروسات الكمبيوتر:

الفيروسات ما هي إلا قنبلة موقوتة تطيح بالبرامج والمعلومات أو بأداء الكمبيوتر فيكون غير قادر على العمل وذلك بشل قدرته على التعامل مع البرامج والنظم والبيانات الموجودة بداخله أو على شبكة الإنترنت ويطلق أهل الخبرة في مجال جرائم الكمبيوتر على الفيروسات اسم البرمجيات الماكرة إذ أنها جميع البرامج التي من شأنها أن تتسلل إلى نظام الكمبيوتر ويكون ذلك دون رضا أو معرفة صاحب الجهاز ومن أهم خصائص تلك الفيروسات عدم القدرة على التخلص منها إلا بإزالة معلومات أو برامج هائلة لذلك تحدث تلك البرمجيات الماكرة خسائر.

قد أفادت وكالة الاستخبارات الأمريكية FBI بأن جرائم الكمبيوتر التي تقع على الكمبيوتر أو على شبكة المعلومات العملاقة والتي يكون مضمونها إطلاق فيروسات وبرامج تجسس تكبد الشركات الأمريكية ٦٧,٢ بليون دولار سنوياً.

ذلك أن FBI قد توصلت إلى تلك النتائج من خلال مطالعة نتائج استطلاع شمل ٢٠٦٦ شركة.

وقد توصلت إلى نتيجة مقدارها أن متوسط خسائر كل شركة يزيد على ٢٤ ألف دولار أمريكي بينما بلغ إجمالي خسائر الاستطلاعات ٣٢ مليون دولار أمريكي.

وخلصت تلك الدراسة إلى أن أكثر الجرائم التي تقع الحاسبات وتصيبها بأضرار بالغة هي الديدان الفيروسية والفيروسات وأن سرقة أجهزة الكمبيوتر والاحتياال المالي واختراق الشيكات تأتي في المؤخرة.

ونخلص مما تقدم إلى أن الفيروسات هي عبارة عن برنامج حاسب آلي مثل أي برنامج تطبيقي آخر ولكن يتم تصميمه بواسطة أحد المخربين بهدف محدد وهو إحداث أكبر ضرر ممكن بنظام الحاسب الآلي.

والملاحظ أن مصمم برنامج الفيروس دائما يعطي هذا البرنامج قدر من القدرة علي ربط نفسه بكافة البرامج الأخرى الموجودة علي أجهزة الحاسبات الآلية ويكون لذلك البرنامج الفيروسي القدرة علي إنشاء نفسه وإعادة نسخ نفسه بصورة تقنية تبدو كعملية تكاثر وتوالد لفيروس عضوي الفارق بين الفيروس الذي يصيب الحاسب والفيروس العضوي الذي يصيب الكائن الحي:

أن فيروس الحاسب مثله مثل الفيروس العضوي في صفة القدرة علي الاختراق ويتسبب في تغيير خصائص الحاسب والبرامج التي عليه ويتوالد ويتكاثر بإعادة نسخ نفسه ملايين المرات أي قدرته علي التكاثر ذاتياً *itself* . Reproduce

ومن الجدير بالذكر أن الفيروس الحاسبي مثله مثل الفيروس العضوي في أنه قد يضل كامن لا يظهر مباشرة بل ينتظر إلي أن يحدث حدث ما ينسخه فيظهر ويقضي علي البرامج أو يتلفها فور ظهوره.

ويتماثل ذلك الفيروس مع الفيروس العضوي بقدرته علي تغيير شكله حتى لا يكتشفه أحد إذ هو يتخفي في صورة عكس الصورة التي يظهر بها، أهداف الفيروس هو التوالد والتكاثر وإصابة أكثر عدد ممكن من الحاسبات ليس علي مستوى الدولة الواحدة بل مستوى القارات في أقل وقت ممكن ويحدث مع انتشاره آثار تدميرية في أنظمة تشغيل الحاسبات الآلية ينتج عنها أضرار فادحة وكبيرة سواء من الناحية المادية أي لذات الأجهزة أو للبرامج المعلوماتية أيا كان نوعها وكل ذلك يتم في وقت قصير الأمر الذي لا يعطي

فرصة لعلاج الأمر ومن أمثلة الفيروسات فيروس أحبك الذي خرج من الفلبين في ٤ مايو عام ٢٠٠٠ وكذلك فيروس مليسا Melisa .

فمثلا فيروس أحبك ينتشر من خلال استخدام أنظمة الرسائل الفورية Amil ويستهدف الفيروس تدمير أنظمة أجهزة الحاسبات التي تعمل بنظام الوندوز الذي تنتجه شركة مايكروسوفت العملاقة ويظهر الفيروس في البريد الإلكتروني في صورة رسالة بعنوان I love you .

التي يشاهدها مستخدم الحاسب فيحول مستخدم الحاسب معرفة من يحبه دون أن يدرس الأمر ويفحصه فيقوم بفتح الرسالة وبمجرد فتحها ينتشر فيروس أحبك في جميع العناوين المسجلة لدى مستخدم الحاسب في بريده الخاص وكذلك تنتشر في كافة الرسائل المرسلة من هذا الجهاز إلي الأجهزة الأخرى مصيبة إياها بذات الفيروس الذي يصيب بريد الآخرين بطريقة تكاثرية ومتوالدة ومن أفكار فيروس I love you وهذا الفيروس له قدرته علي تدمير المحتويات المعلوماتية الموجودة علي الحاسب.

أما الفيروس الآخر الذي لا يقل عنه شهرة فهو فيروس تشير نوبيل وقد أطلق عليه هذا الاسم لكي يذكر الآخرين بما أحدثته فاجعة تشيرنوبيل النووي الروسي الذي انفجر محدث آثار تدميرية أصابت المنطقة الذي انفجر فيها وكذلك المناطق المتاخمة معها وكان من الآثار هذه استحالة الحياة في تلك المناطق لتلوثها بالإشعاع النووي في أوكرانيا في ٢٦/٤/١٩٨٦ أما فيروس تشيرنوبل فهو ينشط في ذات التاريخ الذي حدث فيه فاجعة تشيرنوبل أي يوم ٢٦/٤ من كل عام ويؤكد الخبراء أن فيروس تشيرنوبل بالغ الدقة ينتقل عبر شبكة الإنترنت فيتسلل إلي أجهزة الكمبيوتر حيث يقوم بتدمير كافة المعلومات المخزنة علي الحاسب وهو ينشط في يوم ٢٦ إبريل من كل عام.



وكذلك هناك فيروس آخر يصيب أجهزة الحاسوب في يوم ٢٦ مارس من كل عام وهو فيروس مايكل أنجلو حيث يقوم هذا الفيروس بمسح كافة المعلومات المخزنة علي القرص الصلب لكافة الأجهزة المصابة به وهو ينشط في يوم عيد ميلاد الفنان الشهير لعصر النهضة في روما مايكل أنجلو. وهناك أيضا فيروس آخر يصيب الحاسبات يطلق عليه حصان طروادة.

Troian Horse، وهو علي غرار الفكرة التي استعملها المحاربون القدماء عندما قنموا إلي أعدائهم هدية لتعبر لهم عن السلام في صورة حصان كبير كان يقع بداخله كافة الجنود الأعداء الذين استطاعوا فك حصار طروادة المدينة الحصينة التي لم يستطيع أحد دخولها أو الولوج فيها- إذ بمجرد دخول هذا الحصان الضخم بما يحويه من محاربون أعداء تمكنوا في خلال ساعات من إسقاط تلك المدينة المنيعه.

وفي وقت السلم فإن الأمر يختلف إذ تخدم تلك الشبكات المعصورة بأكملها وتجعلها مثل قرية صغيرة الأمر الذي يوقر الجهد والوقت والعمل ويجعل أمور كثيرة سهلة وميسورة لم تكن أبداً كذلك قبل اختراع الحاسب الآلي وبرامجه التي تستخدم أعلي التقنيات في الاتصال والمعلوماتية إذ أن شبكات أجهزة الحاسبات تخدم كافة مجالات الحياة ولا سيما الاقتصادية منها في الصناعة والزراعة والإدارة والتجارة وفي كافة أجهزة الدول الحكومية الأمر الذي يسهل علي المتعاملين مع الإدارات الحكومية العمل ويقضي علي البيروقراطية والفساد.

وتلك الجرائم تشمل الاعتداء الذي يقع علي شبكة الإنترنت وكذلك تشمل الاعتداء علي المواقع الموجودة علي الشبكة وذلك باختراقها أو تدميرها وقد يكون تلك المواقع شخصية وقد تكون رسمية أو الاستيلاء علي تلك المواقع وإغراقها بالرسائل الفيروسية وانتهاك خصوصية الغير وذلك بمعرفة أسرارهم

المالية والاجتماعية والاقتصادية بهدف استغلالها والإضرار بالغير من الناحية المادية والمعنوية.

وقد يستخدم المهاجم في هجومه ما يعرف بالقنبلة المنطقية وهي عبارة عن برنامج له القدرة علي تدمير كافة المعلومات.

**والمهاجم له أساليب كثيرة في مهاجمة الغير ومن تلك الأساليب:**

#### **- الاقتحام أو التسلل.**

وبذلك بإرسال رسالة إلي البريد الشخصي والتسلل إلي برنامج الحاسب ومعرفة كلمة السر Poss word حتى يكون هناك اختراق يستطيع المهاجم التجسس علي أعمال مستخدم الكمبيوتر وكذلك يستطيع نسخ أعمال مستخدم الكمبيوتر دون علمه فيعرف رقم بطاقة الائتمان أو التوقيع الإلكتروني.

ويستطيع قراصنة الإنترنت اقتحام الصفحة الرئيسية وأن يضعو عليها صور أو شعارات أو إرسال سب وقذف لأشخاص محددين كما حدث بالنسبة لصفحة رئيسية لبنك وجريدة وقد استطاع البعض التسلل إلي الصفحة الرئيسية لإحدى القواعد العسكرية أثناء حرب الخليج وكان ذلك بفعل مراهقين يلهون وكان الاتجاه في أول الأمر إلي اعتبارهم إرهابيين.

كما حدث أن تسلل البعض إلي الصفحة الرئيسية التي تحكم تغذية الكهرباء إلي معظم أنحاء ولاية كاليفورنيا.

وفيرس حصان طروادة أخذ مبرمجه ذات الفكرة اليونانية القديمة في إخفاء الجنود داخل الحصان الخشب إذ هو يخفي البرنامج الفيروسي داخل الرسالة الجميلة.

ويستعرض دائماً هؤلاء الهواة أو محترفي تخريب الكمبيوتر وشبكة الإنترنت قدرتهم العلمية علي خلق المشكلة بل وقدرتهم علي حلها أيضا بمقابل يحدونه في بعض الأحيان.

والملاحظ أن استخدام فيروسات الحاسب غير مجرمة في الحروب طالما كل شيء مباح للفوز على العدو لذلك تجد دائما العسكريون يطورون تلك الفيروسات لاستخدامها في الحروب.

- كما يلجأ البعض من هؤلاء الأشخاص الذين يطلق البعض عليهم قراصنة الكمبيوتر إلى إرسال مئات الرسائل إلى البريد الإلكتروني EmAil. حيث يؤدي ذلك إلى إغراق صندوق البريد الذي لا يستطيع استقبال أية رسائل أخرى وتكون تلك الرسائل فيروسية أو محملة بملفات كبيرة لا يستطيع البريد الإلكتروني استيعابها.

- أو قد يرسل مئات الرسائل دفعة واحدة أو جملة واحدة.

#### ماهية وطبيعة التطورات المعاصرة في البيئة الاقتصادية العالمية:

إن التطورات الهائلة التي حدثت خلال السنوات الأخيرة يمكن إرجاعها إلى عنصرين رئيسيين، هما تطور التقنية، وتهيئة البيئة العالمية المناسبة. يتمثل العنصر الأول في مدى التطورات الهائلة في تكنولوجيا المعلومات والاتصالات، في حين يتمثل العنصر الثاني في توفير وإتاحة وتهيئة البيئة لانتقال كافة التغيرات ونفاذها من مكان لآخر بدون مواجهة أية حواجز جغرافية، وهو ما يعرف بعولمة السوق أو الاقتصاد. ولذلك إن تخلف أي من هذين العنصرين لما شاهدنا التطورات الكبيرة والمتسارعة خلال الفترة الأخيرة.

#### صورة المعلومات وتطورات المجتمع الإلكتروني:

لقد أصبحت المعلومات في بيئة اليوم ترتبط بمختلف جوانب الحياة، وتمثل ركيزة نشاط الإنسان الاقتصادي والاجتماعي والثقافي والسياسي، وتتيح المعرفة بالواقع ومشكلاته وأبعاد هذه المشكلات، بل أنها أصبحت تتيح إمكانية اتخاذ القرارات في كافة المجالات تقريبا. وعلى الرغم من تعدد المصطلحات التي تطلق على ثورة المعلومات، إلا أنه يات هناك نوع من

الاتفاق حول مسمى المجتمع الإلكتروني للتعبير عن التقدم التكنولوجي الهائل في تقنيات المعلومات.

وتتمثل المكونات الرئيسية للمجتمع الإلكتروني في ثلاثة مكونات رئيسية، هي الحاسبات والاتصالات والشبكات والوسائط المتعددة<sup>(١)</sup>.

هذا ولقد كان من الملاحظ خلال السنوات الأخيرة أن ثورة التقنية العالية ترتبط وتخلق مزايا ومنافع في كل مشروع أو صناعة، بحيث احتلت أجهزة الكمبيوتر وشبكات الاتصالات موقعا رئيسيا داخل العمليات والصفقات اليومية لمعظم المشاريع والمؤسسات، الأمر الذي جعلها محددًا رئيسيًا لتنافسيتها للسيطرة على الأسواق.

لذلك، فقد يكون من الصعوبة محاولة حصر محتوى الخدمات والمنافع التي يقدمها المجتمع الإلكتروني. إلا أنه يمكن فقط الوقوف على الخطوط العريضة لهذا المحتوى، والتي تتمثل في الاتصالات الرقمية، والمنزل الإلكتروني، وإتاحة الموسوعات العلمية والمعلوماتية على الخط، والنشر الإلكتروني، والتعليم والتدريب الإلكتروني، وتوظيف التقنية في النشاط المهني، والتوظيف الإلكتروني، والأعمال الإلكترونية، والتجارة الإلكترونية، والمال والبنوك الإلكترونية، والحكومة الإلكترونية، والقرار الإلكتروني، والعصيان المدني الإلكتروني Electronic Civil Disobedience (ECD)<sup>(٢)</sup>.

(١) يونس عرب (٢٠٠١)، لعالم الإلكتروني: الوسائل والمحتوي والمزايا والسلبيات: النصين الرابع والسادس، كتاب قانون الكمبيوتر، منشورات اتحاد المصارف العربية، الأردن.  
(٢) المرجع السابق.

## برنامج مكافحة الفيروسات: الأسئلة المتداولة: (١)

س: ما هو برنامج مكافحة الفيروسات؟

ج: تساعد برامج مكافحة الفيروسات في حماية الكمبيوتر من معظم الفيروسات والبرامج الدودية وأحصنة طروادة ومخترقي الكمبيوتر الآخرين غير المرغوب فيهم الذين قد يقوموا بأفعال ضارة. قد يقوموا بحذف الملفات أو الوصول إلى البيانات الشخصية أو استخدام الكمبيوتر الخاص بك في مهاجمة أجهزة الكمبيوتر الأخرى. يأتي برنامج مكافحة الفيروسات مثبتاً على الكمبيوتر الخاص بك أو يمكنك شرائه وتثبيته بنفسك.

س: لماذا ينبغي علي استخدام أحد برامج مكافحة الفيروسات؟

ج: يساعد برنامج مكافحة الفيروسات في الحفاظ على الكمبيوتر الخاص بك آمناً. لا تتس تحديث برنامج مكافحة الفيروسات لديك بانتظام. تتوفر هذه التحديثات عامة عبر الاشتراك بشركة برامج مكافحة الفيروسات.

س: كيف يمكنني معرفة ما إذا كان هناك بالفعل برنامجاً لمكافحة الفيروسات مثبتاً على جهاز الكمبيوتر الخاص بي؟

ج: راجع قائمة برامج من قائمة Start وابحث عن أي برنامج لمكافحة الفيروسات. تقوم العديد من شركات تصنيع أجهزة الكمبيوتر الكبرى بتضمين نسخة تجريبية واحدة على الأقل من إحدى حزم برامج مكافحة الفيروسات الشائعة مثل MzAfee أو Symantec لكن، لا يعني وجود برنامجاً لمكافحة الفيروسات مثبتاً على الكمبيوتر الخاص بك، أنه قيد التشغيل، وأنه يقوم بتحديث نفسه بانتظام.

(١) <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.mspx>

س: أين يمكنني الحصول علي برنامج مكافحة الفيروسات إذا لم أجده مثبتاً؟

ج: إذا لم يكن لديك برامج مكافحة الفيروسات مثبتاً، فيمكنك الحصول عليه من إحدى الشركات المتعددة. للحصول علي العروض الخاصة المتعلقة بحزم مكافحة الفيروسات وجدران الحماية، قم بزيارة برامج متعلقة بالأمان: برامج للتحميل وبرامج تجريبية <sup>(١)</sup>

س: لدى بالفعل برنامج مكافحة فيروسات مثبتاً، ولكنني أرغب في تثبيت برنامج لمكافحة الفيروسات من شركة مختلفة. هل يمكنني القيام بذلك؟

ج: إذا كان لديك بالفعل برنامج مكافحة فيروسات مثبتاً، ولكنك ترغب في تثبيت منتج جديد من شركة مختلفة، فقم بإزالة برنامج مكافحة الفيروسات الحالي قبل تثبيت البرنامج الجديد. قد يؤدي ترك الإصدار السابق مثبتاً إلي حدوث تعارضات في النظام.

س: كيف يمكنني المحافظة علي تحديث برنامج مكافحة الفيروسات؟

ج: إن وجود برنامج قديم لمكافحة الفيروسات يعني وجود برنامج غير فعال لمكافحة الفيروسات. يعتمد عمل برنامج مكافحة الفيروسات علي التحديثات الدورية في الحماية من أحد التهديدات، إذا لم تقم بالاشتراك لدى إحدى الشركات للحصول علي التحديثات، فربما يكون الكمبيوتر الخاص بك عرضة لهجمات البرامج الضارة. سوف تجد هنا بعض التلميحات للتأكد من أن برنامج مكافحة الفيروسات المثبت لديك يتم تحديثه دورياً:

- اشترى اشتراكاً سنوياً من إحدى شركات برنامج مكافحة الفيروسات وتأكد من أن برنامج مكافحة الفيروسات لديك محدث وفعال. إذا قمت بشراء

(١) <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.mspx>



أحد الاشتراكات، فإن أغلب برامج مكافحة الفيروسات تقوم بتحديث نفسها تلقائياً عندما تتصل بالإنترنت<sup>(١)</sup>

- للتأكد من أن برنامج مكافحة الفيروسات لديك محدث، افتح برنامج مكافحة الفيروسات لديك من القائمة Start أو منطقة الإعلام الموجودة في شريط المهام وابحث عن حالة التحديث، وإذا كنت غير متأكد من تحديث برنامج مكافحة الفيروسات، فانتصل بموفر برامج مكافحة الفيروسات.

س: أرغب في تثبيت أحد البرامج الجديدة، ولكن تخبرني عملية التثبيت بضرورة إيقاف تشغيل برنامج مكافحة الفيروسات، هل هذا الفعل آمن؟

ج: ينبغي عليك في بعض الأحيان إيقاف تشغيل برنامج مكافحة الفيروسات المثبت لديك عند تثبيت أحد البرامج الجديدة. لا تنس إعادة تشغيل برنامج مكافحة الفيروسات مرة أخرى بعد الانتهاء من عملية التثبيت.

س: لقد عطلت بعض الإعدادات الموجودة في برنامج مكافحة الفيروسات المثبت لدى، ولكنني غير متأكد الآن من ضرورة قيامي بذلك. ما هي أكثر الإعدادات أهمية التي ينبغي تمكينها؟

ج: الإعدادات التالية هي الإعدادات التي يتم تمكينها بشكل افتراضي عندما تقوم بتثبيت برنامج مكافحة الفيروسات ولا ينبغي عليك تعطيلها لفترات زمنية طويلة، إذا دعت الحاجة إلي تعطيل هذه الإعدادات لتثبيت أحد البرامج الجديدة أو لأي سبب آخر، فتأكد من إعادة تمكين هذه الإعدادات في أقرب وقت ممكن.

- ينبغي القيام بتمكين خيار فحص "On- access" أو "real-time" إن القيام بتعطيل هذا الخيار يمكن أن يعرض جهاز الكمبيوتر الخاص بك للتهديدات. ينبغي أن يظهر رمز في منطقة الإعلام من شريط

(١) <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.mspx>

المصمّم للإشارة إلى تمكين هذا الإعداد. ربما تري التفاصيل المتعلقة بإعدادات  
مكافحة الفيروسات الخاص بك عند الضغط علي هذا الرمز. (انقر  
على الرمز المتعلق ببرنامج مكافحة الفيروسات المثبت علي جهازك في قائمة  
البرامج الموجودة في قائمة Start للحصول علي نفس المعلومات).

- ينبغي ضبط برنامج مكافحة الفيروسات للقيام بعمليات فحص مجدولة  
نقصرص الثابت الخاص بك.

- ينبغي عليك تهيئة برنامج مكافحة الفيروسات المثبت لديك ليقوم  
بفحص البريد الإلكتروني افتراضيا.

س: أين يمكنني الحصول علي معلومات إضافية حول برامج مكافحة  
الفيروسات؟

ج: قم بزيارة الفيروسات والبرامج الدودية لمزيد من التفاصيل حول  
مكافحة الفيروسات.

ما هي برامج التجسس؟<sup>(١)</sup>

إن "برنامج التجسس" هو مصطلح عام يستخدم لوصف البرامج التي تقوم  
بسلوكيات معينة، كعرض الإعلانات، أو جمع المعلومات الشخصية، أو تغيير  
تكوين الكمبيوتر، ويحصل ذلك عادة من دون الحصول علي موافقتك أولا  
بالصورة الملائمة.

غالبا ما يتم إقران برامج التجسس بالبرامج التي تعرض الإعلانات  
(وتحمل اسم برامج الإعلانات المتسللة)، أو بالبرامج التي تتعقب المعلومات  
الشخصية أو الحساسة.

(١) <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.msp>

ولكن، لا يعني ذلك أن كافة البرامج التي توفر الإعلانات أو تتعقب نشاطاتك عبر إنترنت هي سيئة، فمثلاً، قد تقوم بالتسجيل للاشتراك بخدمة موسيقي مجانية، ولكن تقوم بـ "نفع" ثمن الخدمة عبر الموافقة علي تلقي إعلانات هادفة، إذا فهمت الشروط ووافقت عليها، تكون قد قررت أن تلك هي عملية تبادل عادلة، قد توافق أيضاً علي أن تتعقب الشركة نشاطاتك عبر إنترنت لتحديد الإعلانات التي ستعرضها عليك.<sup>(١)</sup>

أما الأنواع الأخرى من برامج التجسس، فتجري تغييرات مزعجة في الكمبيوتر قد تتسبب بإبطاء الجهاز أو بتعطيله.

فتستطيع هذه البرامج تغيير الصفحة الرئيسية أو صفة البحث لمستعرض ويب، أو إضافة مكونات إضافية إلي المستعرض لا تحتاج إليها أو لا ترغب فيها. كذلك تصعب هذه البرامج عليك تغيير الإعدادات وإعادتها إلي ما كانت عليه في الأصل.

وفي كافة الحالات، الأهم هو ما إذا كانت قد فهمت (أنت أو مستخدم الكمبيوتر) أو لم تفهمك ما سيقوم به البرنامج، ووافقت علي تثبيته علي الجهاز.

ثمة طرق عديدة تستطيع من خلالها برامج التجسس أو البرامج الأخرى غير المرغوب فيها الوصول إلي الكمبيوتر. وتكمن إحدى الحيل الشائعة في تثبيت البرنامج بشكل سري، خلال تثبيت برنامج آخر ترغب فيه، مثل برنامج مشاركة ملفات الموسيقى أو الفيديو.

كلما تقدم بعملية تثبيت علي الكمبيوتر، احرص علي قراءة كافة المعلومات التي تم الإصاح عنها بعناية، بما في ذلك اتفاقية الترخيص وبيان الخصوصية. وأحياناً، يتم توثيق تضمين برنامج غير مرغوب فيه في تثبيت برنامج معين، ولكن قد يظهر في نهاية اتفاقية الترخيص أو بيان الخصوصية.

(١) <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.msp>

## مراقبون يحصلون علي معلومات نووية: (١)

أفاد مسئولون في ولاية كاليفورنيا بأن مراقبين استولوا، عبر شبكة الإنترنت، علي آلاف شفرات الدخول إلي مواقع خاصة، وتمكنوا من التسلل إلي شبكات معلوماتية تابعة لمختبرين أمريكيين يعملان في إطار برنامج الأسلحة النووية.

وأوضحت جان هوجنسون، رئيسة قوة مكافحة جرائم التكنولوجيا المستطورة في ساكرامنتو فالي، بولاية كاليفورنيا، أن هؤلاء المتسللين وهم خمسة شبان تتراوح أعمارهم ما بين ١٥ و ١٧ عاما، تمكنوا من الدخول إلي ٢٦ موقعا خاصا في الولايات المتحدة وخارجها.

وأضافت أنه كانت بحوزة المتسللين لائحة تضم شفرات دخول مائتي ألف مستعمل، وأنهم تمكنوا من استخدام كلمات السر لتصفح الشبكتين الإعلاميتين لمختبري سانديا وأوك ريدج الأمريكيين.

ويستخدم مختبر سانديا لتصميم كافة المكونات غير النووية للأسلحة النووية الأمريكية، في حين أنشئ مختبر أوك ريدج عام ١٩٤٣ لإنتاج البلوتونيوم الذي استعمل في إنتاج أولى الأسلحة النووية الأمريكية.

وأوضحت هوجنسون أن المتسللين لم يتمكنوا من الإطلاع علي محتوى شبكتي المختبرين، إلا أن مسؤولين فيدراليين وصفوا أنشطة هؤلاء المراقبين بأنها زيارات غير مرغوب فيها وعلي الرغم من عدم اعتقال هؤلاء الشباب، فإن السلطات قد اتصلت بهم.

ويأتي هذا الحدث في خضم مجموعة من عمليات التسلل الإلكترونية المثيرة، حيث أعلن الإثنين الماضي أن متسللين استولوا علي آلاف الأرقام

(١) <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.msp>

السرية لبطاقات الائتمان من أحد بائعي الموسيقى علي شبكة الإنترنت، وحاول المتسللون إبتزاز الموقع حيث طلبوا إعطاءهم مائة ألف دولار أمريكي، وإلا سينشرون الأرقام علي شبكة الإنترنت. وفعلًا استخدمت بعض البطاقات بشكل غير قانوني في عمليات شراء قيمتها ألف دولار.<sup>(١)</sup>

وقالت وزيرة العدل الأمريكية، جانت رينو، إنه بالرغم من المنافع الجمة التي يمكن الإنترنت من جنيها، فإنه يتضمن جانبًا سلبيًا يتمثل في عمليات الاختراق، والاتلاف وبث الفيروسات، داعية إلي التصدي لمثل هذه الجوانب السلبية.

وكان استطلاع لمكتب التحقيقات الفيدرالي الأمريكي، شمل خمسمائة شركة، قد توصل إلي أن نسبة ٦٢ في المائة منها أبلغت العام الماضي عن تجاوزات لسلامة الكمبيوتر.

طرق للمساعدة علي تجنب الأطفال قرصنة الملفات عبر إنترنت:

تكن القرصنة عبر إنترنت في نسخ المواد المحمية بقوانين حقوق النشر، ومشاركتها بصورة غير قانونية من أجل استخدام مهني أو شخصي.

ويشمل ذلك تنزيل الموسيقى أو الأفلام أو الألعاب من دون الحصول علي إذن من مالك حقوق النشر، إضافة إلي مشاركة نسخ الموسيقى والأفلام والألعاب والبرامج التي تملكها.

إذا كان أطفالك يقومون بقرصنة ملفات رقمية، فقد تكون عرضة لغرامات باهظة أو لرسوم جزائية أخرى، وقد يعرض ذلك لـ فيروسات وبرامج تجسس وبرامج أخرى غير مرغوب فيها.

(١) <http://www.microsoft.com/middleeast/arabic/athome/security/online/netiquette.msp>

إليك أربع طرق لمساعدتك علي منع أطفالك من إجراء عمليات تنزيل غير قانونية.

#### ١- حذر الأطفال من المخاطر:

القرصنة هي سرقة بكل بساطة، وكلما أدرك أطفالك هذا في وقت مبكر، كلما كان ذلك أفضل.

كما نعلمون علي الأرجح، أحيانا لا يكفي فقط أن تقول لطفل بأن ثمة خطب ما، وقد يفيد في هذا الإطار التحدث عن العواقب.

في ما يلي بعض الجزاءات التي قد تكون أنت أو أطفالك عرضة لها، في حال قاموا بتنزيل الموسيقى بشكل غير قانوني:

- بموجب حقوق الطبع والتأليف والنشر في الولايات المتحدة، قد تتم مطالبتك بدفع غرامة تصل إلي ٣٠٠٠٠ دولار (قد تختلف الغرامات حسب الدولة).

- قد تم مصادرة الكمبيوتر المنزلي الخاص بك والملفات والأقراص ذات الصلة.

- قد يعرض ولدك الكمبيوتر لخطر الفيروسات.

- قد يعرض أطفالك الكمبيوتر لخطر برامج التجسس أو برامج أخرى غير مرغوب فيها.

#### ٢- راقب أنشطة الأطفال علي الكمبيوتر:

بعد شرح مخاطر القرصنة لأطفالك، قد تود الاستمرار في مراقبة نشاطهم، إليك تلميحات من شأنها مساعدتك:

- ضع الكمبيوتر في غرفة مركزية ضمن المنزل، حدد أوقاتا معينة لاستخدام الكمبيوتر وعدم استخدامه من قبل الأطفال، وتأكد من أنهم قد فهموا أيًا من النشاطات مقبولا وأيًا منهم غير مقبول.



- بالرغم من أن خدمة ويب غير مصممة لتكون بدلا لتدخل الأهل، إلا أنها تستطيع مساعدتك علي مراقبة ما يفعله أطفالك علي إنترنت، فتسمح لك بتعاقب نشاطاتهم علي إنترنت.

**اختبر إعدادات أمان عائلة Windows Vista المضمنة في أحدث نظام تشغيل من Microsoft أو أمان عائلة Windows Live**  
تلميح: اقرأ ١٠ أمور بإمكانك تعلمها لأطفالك لتعزيز أمانهم علي إنترنت لتعلم المزيد من الطرق التي من شأنها مساعدتك علي المحافظة علي أمان أطفالك عند اتصالهم بإنترنت.

٣- امنح ولدك حساب مستخدم محدود الحقوق:

يسمح لك **Windows Vista** أو **Windows Live** — إنشاء حسابات مستخدمين متعددة للكمبيوتر. يستطيع كل مستخدم تسجيل الدخول بشكل مستقل وله ملف تعريف فريد بالإضافة إلي "سطح المكتب" ومجلد "المستندات" خاصين به.

بصفته أحد الوالدين، تستطيع أخذ حساب المسؤول الذي يسمح لك بالتحكم الكامل بالكمبيوتر، ومنح أطفالك حسابات مستخدمين محدودة الحقوق تتضمن إمكانيات تحكم مقيدة تساعد علي إبقاء الأطفال بعيدين عن المشاكل.  
٤- علم أطفالك كيفية التنزيل بشكل قانوني:

هناك العديد من المواقع المختلفة علي ويب حيث تستطيع وأطفالك تنزيل البرامج، والأفلام، والألعاب، والموسيقى مجانا أو بسعر منخفض،،  
مثلا، يقدم **MSN Music** أكثر من مليون مسار لأبرز الأسماء الموسيقية، إضافة إلي فنانين مستقلين وجدد لم يتم اكتشافهم بعد، فكر في منح أطفالك مصروفا خاصا بالموسيقى أو الألعاب أو البرامج الأخرى، فلا يضطرون إلي المخاطرة بتنزيلها بطريقة غير قانونية.

### لماذا ينبغي عليك استخدام جدار الحماية:

عبر إنترنت، يستخدم المتطفلون تعليمات برمجية خبيثة، مثل الفيروسات العالدية والمتنقلة وأحصنة طروادة، في محاولة منهم للعثور على أجهزة كمبيوتر غير محمية.

فبينما بعض الهجمات تؤدي إلى إزعاجات فقط من خلال الدعايات البسيطة، فإن غيرها يتم إنشاؤها بقصد التسبب في الضرر.

قد تحاول هذه الأنواع الخطيرة حذف معلومات من الكمبيوتر، أو تعطيله، أو حتى سرقة معلومات شخصية، مثل كلمات المرور أو أرقام البطاقات الائتمانية. لحسن الحظ بإمكانك تقليل خطر الإصابة من خلال استخدام جدار حماية.

### كيف اختار جدار الحماية؟

يقوم جدار الحماية بتفحص المعلومات الواردة من إنترنت والصادرة إليه، ويتعرف على المعلومات الواردة من المواقع الخطرة أو تلك التي تثير الشك ويوقفها.

إذا أعادت جدار الحماية بشكل صحيح، فلن يتمكن المتطفلون الذين يبحثون عن أجهزة الكمبيوتر التي لا تتمتع بالحصانة من الكشف عن الكمبيوتر الخاص بك.

تستوفر ثلاثة أنواع أساسية من جدار الحماية، الخطوة الأولى عند اختيار جدار الحماية هي تحديد أي منها هو الأفضل لك. وتشمل الخيارات ما يلي:

- جدران الحماية البرمجية.
- أجهزة التوجيه.
- أجهزة التوجيه اللاسلكية.

بداية، أجب عن هذه الأسئلة وسجل إجابتك:

- ١- كم هو عدد الأجهزة التي ستستخدم جدار الحماية.
  - ٢- ما هو نظام التشغيل الذي ستستخدمه؟ (قد يكون هذا إصدار من Microsoft Windows أو Linux Apple Macintosh)
- هذا كل ما في الأمر، أنت الآن جاهز لتبدأ التفكير في نوع جدار الحماية الذي ترغب في استخدامه. هناك عدة خيارات، وكل منها له إيجابياته وسلبياته.

### جدار حماية ( Windows Vista و Windows XP Service pack 2 فقط )

إذا كنت تستخدم ( Windows Vista أو Windows XP Service pack 2 (SP2) فسيكون لديك جدار حماية مدمج وقد للتشغيل بشكل افتراضي.

لمزيد من المعلومات حول جدار الحماية Windows Firewall الذي يرافق Windows Vista و Windows XP SP2 ، راجع فهم جدار

#### حماية Windows

تلميح: إذا لم تقم بتحميل Service pack 2 فقم بزيارة مقطع حماية الكمبيوتر الشخصي لمعرفة كيفية الحصول عليه.

إذا كنت تستخدم Windows XP واخترت عدم تنزيل Service pack 2 يكون لديك وصول إلى جدار حماية اتصال إنترنت (ICF) المدمج في Windows XP، ولكن يتوجب عليك تشغيله.

ملاحظة: إن جدار حماية Windows وجدار حماية اتصال إنترنت غير متوفرين على شكل حزمة بحد ذاتها، كما أنهما غير متوفرين لأنظمة التشغيل الأخرى (على سبيل المثال Linux Apple Macintosh) أو لإصدارات Windows الأخرى عدا Windows Vista و Windows XP.

## :Windows Live OneCare

Windows Live OneCare كناية عن خدمة أمان شاملة تتضمن جدار حماية إضافيا. فجدار حماية Windows Live OneCare مدار في اتجاهين. مما يعني أنه تتم مراقبة حركة المرور الواردة والصادرة، يتم تحديث جدار الحماية بشكل مستمر للمساعدة علي حمايتك.

لمعرفة المزيد من المعلومات، اقرأ ٥ أسباب لاستخدام Windows Live OneCare للمساعدة علي حماية الكمبيوتر أو تجربة Windows Live OneCare.

### برامج جدران الحماية:

برامج جدران الحماية خيار مناسب لأجهزة الكمبيوتر الفردية، وتعمل بشكل جيد مع أنظمة Windows 98 و Windows ME و Windows 2000. (يشتمل نظام Windows Vista و Windows XP علي جدار مدمج بهما، لذلك لا حاجة لجدار حماية إضافي).

تتوفر برامج جدران الحماية من شركات برامج أخرى. للإطلاع علي العروض الخاصة المتعلقة بحزم مكافحة الفيروسات وجدران الحماية، قم بزيارة [برامج الأمان: صفحة مواد للتحميل وبرامج تجريبية](#).

إيجابيات	سلبيات
لا تتطلب أجهزة إضافية	تكلفة إضافية: معظم برامج جدران الحماية تكلف المال
	لا تتطلب مد أسلاك كمبيوتر إضافية. قد تتطلب التنصيب والتكوين قبل الشروع في استخدامها.
	خيار مناسب لأجهزة الكمبيوتر مطلوب نسخة واحدة عادة لكل فردية. كمبيوتر.

### أجهزة التوجيه:

تعد أجهزة التوجيه اختياراً مناسباً للشبكات المنزلية المتصلة بالإنترنت.

إيجابيات	سلبيات
تتضمن أجهزة التوجيه عادة أربعة منافذ للشبكة كحد أدنى لتوصيل أجهزة الكمبيوتر الأخرى توفر أجهزة التوجيه حماية جدار الحماية للعديد من أجهزة الكمبيوتر	تتطلب مد أسلاك، مما قد يتسبب في حدوث فوضى في محيط سطح المكتب.

### أجهزة التوجيه اللاسلكية:

إذا كان لديك شبكة لاسلكية أو كنت في طور التخطيط لاستخدامها، فستحتاج إلى جهاز توجيه لاسلكي.

إيجابيات	سلبيات
تسمح أجهزة التوجيه اللاسلكية بربط أجهزة الكمبيوتر، وأجهزة الكمبيوتر المتنقل، والمساعدات المكتبية الشخصية، والطابعات بدون أسلاك لجهاز التوجيه اللاسلكية ممتازة لربط أجهزة الكمبيوتر المحمولة بالإنترنت والشبكات.	تثبت الأجهزة اللاسلكية المعلومات باستخدام إشارات الراديو التي يمكن اعتراضها من قبل شخص من خارج المنزل (بوجود المعدات المناسب). قد تضطر إلى دفع ثمن أجهزة إضافية. ليست كل أجهزة التوجيه اللاسلكية مجهزة بجدار حماية مضمن، ولهذا، قد تحتاج إلى شراء جدار حماية مضمن، ولهذا، قد تحتاج إلى شراء جدار حماية بشكل منفصل.

الخطوات التالية: أبدأ باستخدام جدار حماية اليوم:

قد ينشأ عن الاتصال بإنترنت التعرض لمخاطر بالنسبة لمستخدم الكمبيوتر غير الواعي. استخدام جدار حماية يساهم في المساعدة علي تقليل الخطر. إن جدار الحماية هو فقط الخطوة الأولى نحو استعراض إنترنت بشكل آمن، بإمكانك متابعة تحسين أمان الكمبيوتر الخاص بك إذا حافظت علي تحديد البرامج واستمررت باستخدام برنامج لمكافحة الفيروسات وبرنامج لمكافحة برامج التجسس. تعلم المزيد حول الخطوات التي بإمكانك اتباعها للمساعدة علي حماية الكمبيوتر.

كيفية إجراء نسخ احتياطي يدويا أو استخدام أداة النسخ الاحتياطي لـ  
Windows XP:

عندما تقوم بإجراء نسخ احتياطية لمعلوماتك، فإن عملية قص ولصق بسيطة تفي بالمطلوب. أما إذا كنت تستخدم Windows XP، فإن حصولك علي أداة النسخ الاحتياطي يحتاج إلي بضع ثورات فقط. بعد أن تقرر ما هي الملفات التي تريد إجراء نسخ احتياطي لها والمكان حيث تريد تخزين النسخ الاحتياطية يمكنك اتباع الخطوات المذكورة في هذه المقالة لإنشاء نسخ احتياطية لمعلوماتك الهامة.

إنشاء نسخ احتياطية يدويا:

بغض النظر عن إصدار Windows الذي تستخدمه، يمكن إنشاء نسخ احتياطي لأي ملف أو مجلد يدويا باتباع الخطوات التالية:

- 1- انقر بزر الماوس الأيمن فوق الملف أو المجلد الذي تريد إجراء نسخ احتياطي له، ثم انقر فوق نسخ من القائمة.
- 2- الآن، في جهاز الكمبيوتر، يمكنك النقر بزر الماوس الأيمن فوق القرص أو محرك القرص الثابت الخارجي حيث تريد تخزين النسخة الاحتياطية، ثم انقر فوق لصق في القائمة.

هذا كل ما في الأمر، بعد الانتهاء من نسخ كل المعلومات التي تريد إجراء نسخ احتياطي لها علي شكل تخزين خارجي، لا تنس المحافظة علي حمايتها.

#### **Windows XP professional: استخدام أداة المسخ الاحتياطي المضمنة:**

إذا كنت تستخدم Windows XP professional فيمكنك استخدام أداة النسخ الاحتياطي المضمنة لمساعدتك علي إنشاء نسخ عن ملفات، أو إعدادات، أو كل ما هو موجود في جهاز الكمبيوتر لديك، حتى أنه يمكنك استخدام الأداة لإجراء نسخ احتياطي لبعض الملفات وفق جدول تحدده. إليك كيفية البدء باستخدام أداة النسخ الاحتياطي:

١- انقر فوق ابدأ، وشر إلى كافة البرامج.

٢- أشر إلى البرامج الملحقة، ثم إلى أدوات النظام.

٣- انقر فوق النسخ الاحتياطي.

إذا لم يسبق لك أن استخدمت أداة النسخ الاحتياطي، فإن الشاشة الأولى التي ستشاهدها هي إطار الترحيب معالج النسخ الاحتياطي أو الاستعادة. انقر فوق التالي واتبع إرشادات المعالج. للحصول علي دليل مفصل خطوة فخطوة

#### **لاستخدام المعالج، انظر سهولة النسخ الاحتياطي في Windows XP**

#### **Windows XP Home Edition: إضافة أداة النسخ الاحتياطي:**

في حال كنت تستخدم Windows XP Home Edition وتود تثبيت أداة النسخ الاحتياطي، فعليك تحديد موقع قرص Windows XP المضغوط الأصلي أولاً. أضف أداة النسخ الاحتياطي يدوياً إلي الكمبيوتر من القرص المضغوط باتتباع الخطوات التالية:

١- ادخل قرص Windows XP المضغوط في محرك الأقراص، وإذا اقتضى الأمر، في جهاز الكمبيوتر، انقر نقراً مزدوجاً فوق رمز القرص المضغوط لعرض شاشة الترحيب.

٢- علي شاشة مرحبا بك في Microsoft Windows XP، انقر فوق تنفيذ مهام إضافية.

٣- انقر فوق استعراض هذا القرص المضغوط.

٤- في مستكشف Windows، انقر نقرا مزدوجا فوق المجلد ValueAdd وفوق Msft، ثم فوق Ntbackup.

٥- انقر نقرا مزدوجا فوق Ntbackup. Msi لتثبيت أداة النسخ الاحتياطي.

ملاحظة: إذا اشتريت جهاز كمبيوتر وفقه Windows XP Home Edition ولم يكن قرص Windows XP المضغوط الأصلي متوفرا لديك، فعليك الاتصال بالشركة المصنعة للكمبيوتر أو زيارة موقع هذه الشركة علي ويب للحصول علي مزيد من المعلومات. كما يمكنك استخدام برنامج النسخ الاحتياطي المنفصل الذي تشتريه عبر الإنترنت، أو من متجر، أو Windows Live Onecare beta.

### Windows Live Onecare Backup and Restore

Windows Live Onecare عبارة عن خدمة من Microsoft

تساعدك علي حماية الكمبيوتر وتوفر أداة نسخ احتياطي مضمنة Windows Live Onecare هو حاليا في مرحلة Beta ويمكن تجربته مجانا. لتعلم

المزيد، اقرأ **Windows Live Onecare Backup and Restore**

كيفية اختيار شكل تخزين خارجي للنسخ الاحتياطي للملفات:

يشير التخزين الخارجي إلي تنسيق لتخزين البيانات غير مثبت بشكل دائم في الكمبيوتر، علي سبيل المثال، الأجهزة كالملفات المضغوطة من نوع محركات Zip ومحركات الأقراص المحمولة Flash والأقراص المضغوطة وحتى خدمات ويب.



## أنواع التخزين الخارجي:

سواء كنت تستخدم الأداة المساعدة للنسخ الاحتياطي لـ Windows XP أو أي برنامج نسخ احتياطي آخر، فأنت بحاجة إلى وسيلة لتخزين النسخ الاحتياطية.

إذا أمكن، استخدم نظام التخزين المحمول، إحدى أفضل الوسائل لحماية نسخك الاحتياطية هي تخزينها في مكان آخر غير جهاز الكمبيوتر، في ما يلي بعض أجهزة التخزين والمواقع التي ننصح بأخذها بعين الاعتبار.

أنواع التخزين	ما هي	إيجابيات	سلبيات
<b>المحركات الخارجية</b>	محرك أقراص من نوع Zip هو محرك أقراص يستخدم أقراص من نوع Zip قابلة للإخراج لحفظ أكثر من مئات الميغا بايت من البيانات	- يتضمن برنامج النسخ الاحتياطي. - خيارات نطاق التخزين. - محمول.	يجب أن تستثمر في الأجهزة وفي بعض الحالات الأقراص أيضا.
<b>الأقراص المضغوطة القابلة لإعادة الكتابة (CD-RW).</b>	إن CD-RW هو قرص مضغوط بإمكانك نسخ معلومات إليه في حال كنت تملك محرك	- يقدم العديد من أجهزة الكمبيوتر الحديثة محرك أقراص مضغوطة قابلة لإعادة الكتابة (CD-RW) في حال لم يكن	- عليك شراء محرك أقراص مضغوطة قابلة لإعادة الكتابة (CD-RW) في حال لم يكن

أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) لنسخ الملفات إلى الأقراص المضغوطة.	أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) - اختصار لـ "read- write"	أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) - تتسع الأقراص المضغوطة القابلة لإعادة الكتابة (CD- RW) ما يصل إلى ٧٠٠ ميغا بايت. - محمول. - من الممكن استخدام أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) وتقد ملفات النسخ الاحتياطي. - يتعذر علي محرركات الأقراص القديمة قراءة الأقراص المضغوطة القابلة لإعادة الكتابة (CD- RW).	أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) - تتسع الأقراص المضغوطة القابلة لإعادة الكتابة (CD- RW) ما يصل إلى ٧٠٠ ميغا بايت. - محمول. - من الممكن استخدام أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) وتقد ملفات النسخ الاحتياطي. - يتعذر علي محرركات الأقراص القديمة قراءة الأقراص المضغوطة القابلة لإعادة الكتابة (CD- RW).
أقراص الفيديو الرقمية القابلة لإعادة الكتابة (DVD- RW) (هو قرص فيديو رقمي)	أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) - اختصار لـ "read- write"	أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) - تتسع الأقراص المضغوطة القابلة لإعادة الكتابة (CD- RW) ما يصل إلى ٧٠٠ ميغا بايت. - محمول. - من الممكن استخدام أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) وتقد ملفات النسخ الاحتياطي. - يتعذر علي محرركات الأقراص القديمة قراءة الأقراص المضغوطة القابلة لإعادة الكتابة (CD- RW).	أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) - تتسع الأقراص المضغوطة القابلة لإعادة الكتابة (CD- RW) ما يصل إلى ٧٠٠ ميغا بايت. - محمول. - من الممكن استخدام أقراص مضغوطة قابلة لإعادة الكتابة (CD- RW) وتقد ملفات النسخ الاحتياطي. - يتعذر علي محرركات الأقراص القديمة قراءة الأقراص المضغوطة القابلة لإعادة الكتابة (CD- RW).

(DVD- RW)	إعادة الكتابة (	أقراص فيديو	بإمكانك نسخ	(DVD- RW)
لنسخ الملفات	رقمية قابلة لإعادة	معلومات إليه في	معلومات إليه في	لنسخ الملفات
إلى أقراص	الكتابة ( DVD-	حالة كنت تملك	حالة كنت تملك	إلى أقراص
الفيديو الرقمية.	الكمبيوتر الخاص	محرك أقراص	محرك أقراص	الفيديو الرقمية.
	بك يتضمن	فيديو رقمية قابلة	فيديو رقمية قابلة	
	أحدها.	لإعادة الكتابة (	لإعادة الكتابة (	
	- قد لا يتضمن	(DVD- RW)	(DVD- RW)	
	المحرك برنامجا	هو اختصار لـ	هو اختصار لـ	
	للتسـخـر	"read- write"	"read- write"	
	الاحتياطي.			
	- من الممكن أن	أكبر.	أكبر.	
	تقوم بطريق	- يـخـزـن القرص	- يـخـزـن القرص	
	الخطأ بالكتابة	الواحد عدة غيغا	الواحد عدة غيغا	
	فوق بيانات	بايت من	بايت من	
	محفوظة في	المعلومات.	المعلومات.	
	قرص الفيديو	- محمول.	- محمول.	
	الرقمي القابل	- من الممكن	- من الممكن	
	إعادة ( DVD-	استخدام أقراص	استخدام أقراص	
	RW) وتنفـذ	فيديو رقمية قابلة	فيديو رقمية قابلة	
	ملفات النسخ	لإعادة الكتابة	لإعادة الكتابة	
	الاحتياطي.	(DVD- RW)	(DVD- RW)	
		عدة مرات.	عدة مرات.	
		- الأقـرـاص	- الأقـرـاص	
		رخصة نسبيا.	رخصة نسبيا.	

محرك أقراص USB	إن محرك أقراص USB هو بمثابة محرك قرص ثابت صغير يتراوح طوله بين ٢ و ٣ بوصات، يمكن توصيله بالكمبيوتر عبر منفذ USB، بإمكانك تنزيل المعلومات فيه لتخزينها	- محمول. - يتسع لما يصل إلى ٣ غيغا بايت من البيانات. - بإمكان حفظ البيانات أو تعديلها أو حذفها قدر ما تشاء. - تبدأ الأسعار نسبيا منخفضة بإمكانك مقارنة مع أسعار الأجهزة.	- يسهل إضاعة محرك USB flash نظرا لصغر حجمه
التخزين والنسخ الاحتياطي عبر إنترنت	تسمح لك خدمة التخزين عبر إنترنت بحفظ الملفات عبر إنترنت. إذ توفر لديك اتصال بإنترنت، فبإمكانك الحصول على الملفات من موقع التخزين عبر	- يقوم بتخزين معلوماتك خارج المنزل والمكتب. - يتضمن مواد تنزيل وبرنامجا للنسخ الاحتياطي. - يقدم مساحة أكبر للتخزين من باقي أجهزة النسخ الاحتياطي	- قد يتطلب منك دفع رسم شهري مقابل النسخ الاحتياطي للملفات وتخزينها (تختلف الأسعار بحسب الموفر والخدمة). - قد لا تتمكن من الوصول إلى ملفاتك في حال

فشل خادم الشركة بإقامة الاتصال.	إنترنت عند الحاجة.	أو المواقع.
- في حال تم التطفل على الشركة، فمن المحتمل أن تتم سرقة معلوماتك.		
- تفقد مورد النسخ الاحتياطي في حال توقفت أعمال الشركة.		

**تلميح:** لإجراء نسخ احتياطي أثناء تنقلك، اعتمد على محركات أقراص USB falsh الصغيرة ذات السعة الكبيرة التي تعلق في حاملة المفاتيح. (للحصول على مثال، قم بزيارة موقع Jomega)

**كيفية مساهمة حساب المستخدم الصحيح في المحافظة على أمان الكمبيوتر:**

هل تعلم ما إذا كنت تستخدم حساب مستخدم محدود الحقوق أم حساب مسؤول في الوقت الحالي؟

إذا كنت تعمل في حساب مستخدم محدود قد تستطيع تخفيف تأثير فيروس أو أي برنامج خبيث آخر.

ولكن إذا وقعت هذه الهجمات وأنت تستخدم حساب مسؤول، فيمكن أن يتمكن المهاجم من الوصول بشكل كامل إلى الكمبيوتر الخاص بك حيث يمكن أن تتراوح النتائج بين حدوث مضايقات إلى نتائج مفعجة.

يشكل استخدام النوع الصحيح للحساب في الوقت المناسب، طريقة ممتازة للمساعدة على حماية الكمبيوتر، كما يعتبر إعداد الحسابات سهلاً.

**ملاحظة:** يقوم Windows Vista افتراضياً بتشغيل برامجك في وضع آمن، في حين أن معظم التطبيقات حاول إجراء عملية يحتمل أن تكون خطيرة وتتطلب امتيازات المسؤول، يطلب Windows Vista موافقتك قبل السماح لذلك البرنامج بالعمل، ويساعد ذلك على تخفيض تأثير الفيروسات وأنظمة التجسس والتهديدات الأخرى. لمزيد من المعلومات، راجع Windows Vista: الأمان.

**اطلع على نوع الحساب الذي تستخدمه حالياً:**

إذا كنت تستخدم Microsoft Windows XP حرك المؤشر فوق الساعة الموجودة في الأسفل، يمين الشاشة، انقر بزر الماوس الأيمن فوق الساعة، ثم انقر فوق ضبط تاريخ/وقت.

- إذا كنت تستخدم حساب مستخدم محدود الحقوق فسوف تظهر رسالة "ليس لديك مستوى الامتياز المناسب لتغيير وقت النظام".

- إذا كنت تستخدم حساب مسؤول فسوف يفتح إطار صغير به عناصر تحكم تساعدك على تغيير الوقت والتاريخ على الكمبيوتر.

**استخدام حساب المستخدم المحدود الحقوق والمسؤول حساب المسؤول:**

حساب المسؤول: نوع الحساب الافتراضي في نظام Microsoft Windows XP تم تخصيص هذا الحساب للسماح لك بما يلي:

- إعادة الكمبيوتر الخاص بك وتثبيت البرامج والأجهزة الأولية الخاصة بك.

- تعيين التفضيلات وإجراء الإصلاحات.

- وإضافة برامج وأجهزة جديدة، مثل برامج مشاركة ملفات الموسيقى أو طابعة.

حساب مستخدم محدود: يوف الوصول إلي وظائف البرامج علي الكمبيوتر، فيتسني لك استخدام الكمبيوتر الخاص بك لإجراء النشاطات الاعتيادية اليومية، علي سبيل المثال، يمكنك أثناء استخدام حساب مستخدم محدود الحقوق استخدام:

- برامج إنترنت والبريد الإلكتروني.

- البرامج الإنتاجية مثل Microsoft PowerPoint و Microsoft Word و Excel.

- برامج الترفيه التي تسمح لك بتشغيل ملفات الموسيقى والفيديو وتحرير الصور، وغير ذلك الكثير.

ملاحظة: يتوفر أيضا حساب "ضيف" - يتمتع بأغلب وظائف حساب المستخدم المحدود ولكنه غير محمي بكلمة مرور، وعلي ذلك يمكن للمستخدم الضيف تسجيل الدخول والخروج بسرعة للقيام بمهام بسيطة، مثل التحقق من البريد الإلكتروني أو استعراض إنترنت.

إعداد حساب مستخدم محدود الحقوق:

ليست حسابات المسؤول مصممة للاستخدام العرضي - فيجب إعداد كل شخص يستخدم الكمبيوتر الخاص بك بواسطة حساب مستخدم محدود يستطيع استخدامه لإجراء أنشطة اعتيادية مثل معالجة الكلمات أو استعراض ويب.

إذا كنت تعاني من إحدى هجمات البرامج الخبيثة، فسيتمكن المهاجم من الوصول بسهولة إلى الكمبيوتر الخاص بك عبر الحساب الذي تستخدم - تمنح الحسابات المحدودة وصولاً محدوداً للمهاجم بينما تمنح حسابات المسؤول المهاجم وصولاً كاملاً.

يمكنك إعداد العديد من حسابات المستخدمين محدودة الحقوق عندما تحتاج إليه لنفسك وللعائلة وحتى الأصدقاء.

١- إعداد حساب مستخدم محدود: تأكد من تسجيل دخولك كمسؤول.

٢- انقر فوق ابدأ، ثم انقر فوق لوحة التحكم.

٣- انقر فوق حسابات المستخدمين، ومن اختر مهمة انقر فوق إنشاء حساب جديد.

٤- في قائمة إجراء، انقر فوق مستخدم جديد.

٥- اكتب اسم المستخدم، ثم انقر فوق التالي.

٦- من اختر نوع الحساب، انقر فوق مستخدم محدود الحقوق ثم انقر فوق إنشاء حساب.

#### التبديل السريع بين المستخدمين:

يوفر نظام Windows XP ميزة تسمى التبديل السريع بين المستخدمين التي تسمح لك بالتبديل بين المستخدمين دون إغلاق البرامج أو إيقاف تشغيل الكمبيوتر الخاص بك.

ويُفضل التبديل السريع بين المستخدمين، تستطيع التبديل إلى حساب المسؤول لبعض الوقت، إذا رغبت في إجراء تعديلات أو كنت بحاجة إلى تثبيت برنامج جديد ثم العودة مرة أخرى إلى حساب المستخدم المحدود من دون مقاطعة أي من العمليتين.



#### إعداد التبديل السريع بين المستخدمين:

يجب أن يكون نظام التشغيل لديك هو Windows XP وأن يكون قد تم بالفعل إعداد حساب مستخدم محدود الحقوق واحد علي الأقل، وألا يكون جزءاً من نطاق شبكة اتصال، بعدها، قم بما يلي:

١- انقر فوق ابدأ وانقر فوق لوحة التحكم، ثم انقر فوق حسابات المستخدمين.

٢- انقر فوق تغيير طريقة تسجيل دخول أو خروج المستخدمين.

٣- حدد مربع اختيار استخدام التبديل السريع بين المستخدمين.

(ملاحظة: قد تحتاج إلي تحديد مربع اختيار استخدام شاشة الترحيب لتمكين مربع اختيار التبديل السريع بين المستخدمين).

٤- انقر فوق تطبيق الخيارات.

#### استخدام التبديل السريع بين المستخدمين:

يمكنك الآن بعد الانتهاء من إعداد الخطوة السابقة، التبديل بين المستخدمين كيفما تشاء عندما تقوم بـ:

١- انقر فوق ابدأ، ثم انقر فوق تسجيل الخروج (أو اضغط علي مفتاح شعار Windows + L).

٢- انقر فوق تبديل المستخدم.

٣- انقر فوق حساب المستخدم الذي تريد تنشيطه.

ملاحظة: بعض ألعاب الكمبيوتر لن تبدأ العمل بشكل صحيح عندما تستخدم التبديل السريع بين المستخدمين - فتتطلب اللعبة وضع القرص الأصلي في محرك الأقراص، حتى لو كان موجوداً مسبقاً.

لمعالجة هذه المسألة بواسطة البرامج، قم بتنزيل SafeDisc Windows XP Fix for Microsoft Games .

بالتفصيل: حول حسابات المستخدمين:

س: هل أواجه خطر التعرض لفيروس أو لبرنامج تجسس أو لبرنامج خبيثة أخرى إذا قمت باستعراض إنترنت في حساب المسؤول، من دون تنزيل أي شيء؟

ج: تعتمد البرامج الخبيثة طرقا عديدة للوصول إلي الكمبيوتر من دون أن تكون قد قمت بأي إجراء، إن الطريقة التي توصي بها لاستعراض إنترنت هي تسجيل الدخول بحساب مستخدم محدود الحقوق.

س: يشغل أطفالي ألعابا علي إنترنت تتطلب تسجيل الدخول في وضع المسؤول. كيف أدعهم يشغلون الألعاب التي يرغبون فيها بأمان أكثر؟

ج: إذا قررت أنه ينبغي عليك أو علي أطفالك تسجيل الدخول إلي مواقع الألعاب التي تتطلب منك أن تكون في وضع المسؤول، فمن الضروري مراعاة ما يلي:

- يجب أن تأتي الألعاب من مصادر موثوقة (مثلا ألعاب موقع MSN). يمكن أن تحتوي مواد تنزيل البرامج "المجانية" التي يطلب منك بعض موفرو الألعاب تنزيلها علي برامج ضارة مرفقة بسرية بهذه البرامج. (يشمل ذلك أيضا وظائف التوصيل" التي تصممها شركات خارجية للاستخدام مع تقنية Microsoft Activex).

- اترك استعراض مواقع ويب الأخرى لوقت لاحق، عند تسجيل الدخول في أحد مواقع الألعاب بحسب المسؤول. ينبغي عليك تشغيل الألعاب فقط وعدم زيارة أي مواقع ويب أخرى. وعندما ترغب في استعراض إنترنت.

فمن الأفضل تسجيل الخروج من حساب المسؤول والدخول بحساب المستخدم محدود الحقوق الخاص بك.

- كن المسؤول عن أطفالك، يمكنك أيضا عدم اضلاع أطفالك علي كلمة مرور المسؤول الخاصة بك، والسماح بتشغيل الألعاب علي إنترنت فقط في ظل إشراف الكبار مع إدراك أنك تستخدم الحساب علي إنترنت لتشغيل اللعبة فقط.

س: هل من طريقة لإعداد حساب بامتيازات كافية خاصة بالمسؤول للسماح لي بتشغيل الألعاب علي إنترنت مع الحد من الأخطار التي قد أتعرض لها؟

ج: إن الأمر ممكن، ولكنه يتطلب نوعا من العمل المعقد وإضافات للبرامج، من أجل تمكين تشغيل البرنامج بالصورة الصحيحة ولم تعتمد Microsoft أيا من الأمرين المذكورين.

إن الطريقة التي نوصي لها لتشغيل ألعاب عبر إنترنت التي تتطلب تسجيل الدخول بحساب المسؤول الخاص بك، هي القيام بتشغيل الألعاب فقط من مصادر موثوق بها واستخدام حساب المسؤول في تشغيل الألعاب فقط، وليس لاستعراض ويب.

#### عولمة الأسواق:

إن القدرة علي التحكم في عدم النفاذ لم يعد موجودا، بحيث أصبح العالم ككل في شرنقة واحدة، حيث تتواجد كافة الدول الآن في عالم يتسم بالقدرة الكبيرة علي التحرك والانتقال للمعلومات والسلع والخدمات والأفراد، والثقافة، وحتى الفيروسات لم يعد بالإمكان إيقافها عند حدود دولة معينة، بشكل مماثل لتنوع الميكروبات التي لا يمكن إيقاف عنوة الإصابة بها من فرد لآخر.

ومنذ بروز مفهوم العولمة أو الكونية في السنوات القليلة الماضية، لا يزال الجدل مستمراً حول حقيقتها وماهيتها، وقد تعددت التعريفات لمفهوم العولمة<sup>(١)</sup>. فأحياناً يعرفها البعض بأنها حرية حركة السلع والخدمات والأيدي العاملة ورأس المال والمعلومات عبر الحدود الوطنية والإقليمية. كما تعرف في أحياناً أخرى بأنها نموذج القرية الكونية التي تربط بين الناس والأماكن ملغية المسافات ومقدمة المعلومات بشكل شامل بلا قيود<sup>(٢)</sup>. وفي أحياناً ثالثة تعرف بأنها نظام عالمي جديد يقوم على العقل الإلكتروني والثورة المعلوماتية القائمة على المعلومات والإبداع التقني غير المحدود دون أدنى اعتبار للحضارات والقيم والثقافات والحدود الجغرافية والسياسية للدول<sup>(٣)</sup>.

وعلى الرغم من تعدد مجالات العولمة من مجالات سياسية وثقافية وتقنية واقتصادية واجتماعية وغيرها، إلا أن مجالات العولمة الاتصالية والاقتصادية لا يزالان يحتلان المجالات الأكثر أهمية ضمن كافة المجالات الأخرى.

بالنسبة للعولمة الاتصالية، فقد أصبح البث القضائي عن طريق الأقمار الصناعية، وبصورة أكثر من خلال شبكة الإنترنت التي تربط البشر في كل أنحاء المعمورة، بما أدى إلى ثورة معرفية هائلة. أما العولمة الاقتصادية، فقد برزت بعد انهيار النظام الاشتراكي، حيث سادت أسس الاقتصاد الحر الذي يركز على اقتصاد السوق والمنافسة، وتعظيم دور القطاع الخاص، واتساع نشاط التجارة بين الدول<sup>(٤)</sup>. الأمر الذي ترتب عليه بروز العديد من المنافع والمزايا الإيجابية لعولمة الأسواق، التي من أبرزها سهولة انتقال

(١) غالب أحمد عطايا (٢٠٠٢)، العولمة وانعكاساتها على الوطن العربي"، ورقة عمل مقدمة على الملتقى التربوي الأول لمواد الجغرافيا والاقتصاد والدراسات الاجتماعية وعلم النفس، الفجيرة، الإمارات.

(٢) علي عبد الله (٢٠٠١)، "التحديات والأبعاد المستقبلية"، العدد ٥٧، مجلة النبأ، مايو.

(٣) محمد إبراهيم عبيد، (٢٠٠٢)، العولمة وأثرها على المستهلك، الندوة الثانية لحماية المستهلك، لجنة حماية المستهلك، مسقط، عمان.

(٤) غالب أحمد عطايا (٢٠٠٢)، العولمة وانعكاساتها على الوطن العربي"، مرجع سبق ذكره.

التكنولوجيا والمعرفة، وتدفق الاستثمار الأجنبي المباشر، وانخفاض تكاليف النقل والاتصالات السلكية واللاسلكية، والاستفادة من التجارة الإلكترونية.

مما سبق يتضح أن العولمة في مضمونها تشتمل على عنصرين رئيسيين، هما التقدم في تكنولوجيا المعلومات والاتصالات، وإزالة الحدود بين الدول. أي أنه ما كان يمكن أن تنتشر عمليات العولمة بدون ذلك التقدم الكبير في هذه التكنولوجيا، والذي تبلور بشكل أساسي في شبكة الإنترنت أو سيادة المجتمع الإلكتروني.

#### دور التطورات المعاصرة في ظهور الجرائم الإلكترونية:

لقد اتضح من التحليل في النقطة السابقة أن التقدم في تكنولوجيا المعلومات والاتصالات يعد أحد الأسباب وراء حدوث عملية العولمة. وعلى الرغم من المزايا والمنافع الإيجابية المرتبة على هذه العولمة وثورة المجتمع الإلكتروني، إلا أنها ساعدت على ظهور وتعزيز أنواع جديدة من الجرائم، من أبرزها جرائم غسيل الأموال، وتهريب المخدرات، واختراق قطاع الأعمال، والإفلاس بالتقليص والغش، والفساد ورشوة الموظفين العموميين وسرقة الملكية الفكرية، والاتجار غير المشروع في الأسلحة وفي النساء والأطفال، والاتجار غير المشروع في الأعضاء البشرية، وسرقة المقتنيات الفنية والثقافية، والغش في التأمين، وجرائم الحاسب الآلي، أو الجرائم الإلكترونية.<sup>(١)</sup>

وتعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطار جسيمة في ظل العولمة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز

(١) تم التوصل إلى تلك الأشكال من الجريمة بناء على المسح الذي أجرته الأمم المتحدة عام ١٩٩٥ عن اتجاهات الجريمة المنظمة.

هذا التقدم بقدراته وإمكاناته أجهز الدولة الرقابية، بل أنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها.

تصنيف وأشكال الجرائم الإلكترونية:

علي الرغم من وجود العديد من التصنيفات لأشكال الجريمة الإلكترونية، إلا أن هذه الدراسة في ضوء تركيزها علي الغش التجاري، فإنها سوف تسعى للتركيز علي تصنيف الجرائم الإلكترونية حسب معيارين رئيسيين فقط، هما معيار مواطن الاختراق، ومدى مساسها بالأشخاص أو الأموال، وذلك كما يلي:

أولاً: تصنيف الجرائم حسب مواطن الاختراق: (١)

- اختراق الأمن المادي: ومن أبرز تلك الاختراقات الاحتيال بمخالفات التقنية، والاحتيال بالانقطاع السلكي، والاحتيال باستراق السمع.
- اختراق الأمن الشخصي للأفراد: ومن أبرز تلك الاختراقات الاحتيال بانتحال صلاحيات شخص مفوض، والهندسة الاجتماعية، والإزعاج والتحرش، وقرصنة البرمجيات.
- اختراق الحماية الخاصة بالاتصالات وأمن البيانات: ومن أبرز تلك الاختراقات الاعتداء علي البيانات، والاعتداء علي البرمجيات.
- الاعتداء علي عمليات الحماية: ومن أبرز تلك الاعتداءات غش البيانات، والاحتيال علي بروتوكولات الإنترنت، والتقاط كلمات السر، والاعتداء باستغلال المزايا الإضافية.

---

(1) لمزيد من التفاصيل، يراجع:  
يونس عرب، أمن المعلومات: ماهيتها وعناصرها واستراتيجياتها.

## ثانياً: تصنيف الجرائم حسب مساسها بالأشخاص والأموال:

- الجرائم التي تستهدف الأشخاص: ومن أبرزها أشكالها الجرائم غير الجنسية التي تستهدف الأشخاص، والجرائم الجنسية.
- الجرائم التي تستهدف الأموال باستثناء السرقة: وتشمل أنشطة اقتحام أو الدخول أو الاتصال غير المرخص به مع نظام الكمبيوتر أو الشبكة، وتخريب البيانات والنظم والممتلكات، وخلق البرمجيات الخبيثة والضارة، ونقلها عبر النظم والشبكات، واستخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص، وغيرها.
- جرائم الاحتيال والسرقة: وتشمل جرائم الاحتيال بالتلاعب بالبيانات والنظم واستخدام الكمبيوتر للحصول على معلومات أو استخدام البطاقات المالية للغير دون ترخيص أو تدميرها، والاختلاس عبر الكمبيوتر أو بواسطته، وسرقة معلومات الكمبيوتر، وقرصنة البرامج وسرقة خدمات الكمبيوتر، وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر.
- جرائم التزوير: وتشمل تزويد البريد الإلكتروني، وتزوير الوثائق والسجلات، وتزوير الهوية.
- جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب، وتشمل تملك وإدارة وتسهيل مشروعات المقامرة على الإنترنت وغيرها.
- جرائم الكمبيوتر ضد الحكومة: وتشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية، وتنفيذ القانون، والإخفاق في الإبلاغ عن جرائم الكمبيوتر، والحصول على معلومات سرية، والإرهاب الإلكتروني وغيرها.

مما سبق يتضح مدى التنوع والاختلاف في حالات وأشكال الجرائم الإلكترونية، والتي تعكس مدى التطور الهائل والمتسارع في تكنولوجيا المعلومات والاتصالات..

#### الملكية الفكرية للمصنفات الرقمية:

#### IP- Digital Works

##### ١- في تحديد المصنفات الرقمية:

##### ١-١ ما هو المصنف الرقمي؟

يمكننا أن ندعي أن تحديد مفهوم المصنف الرقمي سيبقي مثار جدل إلى حين سيما وأنه اصطلاح لم ينتشر بعد في حقل الدراسات القانونية، وربما يحتاج تحديد مفهومه إلى شجاعة فقهية ليطلق أحد ما تعريفا أو توصيفا له ويصار إلى الحوار حوله تمهيدا للوصول إلى رأي غالب أو إجماع حوله، ولسنا من مدعي الريادة في التعامل مع المفاهيم القانونية، لكننا نجد لزاما علينا في هذه الدراسة تحديد أن نحدد مفهوم المصنف الرقمي من واقع دراساته ومعارفنا في حقل دراسات القانون وتقنية المعلومات، وهو مفهوم مطروح للبحث والحوار وفي ذات الوقت الإطار الذي نعتد به لتحديد المصنفات الرقمية.

كلنا يعلم أن علم الحوسبة برمته قام علي العديدين (صفر وواحد)، وأن البرمجيات هي ترتيب لأوامر تتحول إلى أرقام تبادلية، وأن نقل البيانات، رموزا أو كتابة أو أصواتا عبر وسائل الاتصال انتقل من الوسائل الكهربائية والإلكترومغناطيسية والتناظرية إلى الوسائل الرقمية، وأن الصورة وكذا الصوت والموسيقى والنص في أحدث تطور لوسائل إنشائها وتبادلها أصبحت رقمية علي نحو ما أوضحنا في القسم الأول من هذا الكتاب، وحتى عنوان الموقع علي الإنترنت وكذا العنوان البريدي الإلكتروني، تتحول من العبارات



المكتوبة بالأحرف إلى أرقام تمثل هذه المواقع وتتعامل معها الشبكة بهذا الوصف. وصحيح أنه ما يزال هناك تبادل تناظري لا رقمي، فالقارئ الآلي في نظام الكمبيوتر (سكانر) يدخل الرسم وحتى الوثيقة على شكل صورة وليس على شكل نص، وصحيح أن العديد من المواقع على الإنترنت وأغلبها العربية ومواقع اللغات غير الإنجليزية لما تزل تستخدم الوسائل التناظرية في تثبيت المواد على الموقع وليس الوسائل الرقمية. لكن الموقع نفسه، وعبر مكوناته، يتحول شيئاً فشيئاً نحو التبادل الرقمي لما يحققه من سرعة وجودة وأداء فاعل قياساً بالوسائل غير الرقمية<sup>(١)</sup>.

ومن الوجهة القانونية، تعاملت النظم القانونية والدراسات القانونية والقواعد التشريعية مع مصنفات المعلومات بوصفها تنتمي إلى بيئة الكمبيوتر، وهو اتجاه تعبر عنه دراسات فرع قانون الكمبيوتر في النظم المقارنة، وقد شملت هذه المصنفات ابتداء من منتصف أوائل السبعينيات وحتى وقتنا الحاضر ثلاثة أنواع من المصنفات: البرمجيات، وقواعد البيانات وطبوغرافيا الدوائر المتكاملة. وهي مصنفات جاءت وليدة علوم الحوسبة مستقلة عن علوم الاتصال وتبادل المعطيات وشبكات المعلومات، ومع ظهور شبكات المعلومات، والتي ارتبطت في الذهن العامة بشبكة الإنترنت كمعبر عنها وعن التفاعل والدمج بين وسائل الحوسبة والاتصال، ظهرت أنماط جديدة من المصنفات أو عناصر مصنفات تنثير مسألة الحاجة إلى الحماية القانونية وهي: أسماء النطاقات أو الميادين أو المواقع على الشبكة Domain Names، وعناوين البريد الإلكتروني، وقواعد البيانات على الخط التي تضمنها مواقع الإنترنت، تحديداً ما يتعلق بالدخول إليها واسترجاع البيانات منها والتبادل المتعلق بمحتواها الحاصل على الخط،

(١) <http://Arabia.bitsnips.Com/forums/viewtopic.Php?P=1>  
249 & sid = 8 d 5440 aeaec 2e 02188 c 887.

واسترجاع البيانات منها والتبادل المتعلق بمحتواها الحاصل علي الخط، واسترجاع البيانات منها والتبادل المتعلق بمحتواها الحاصل علي الخط، وهو تطور لمفهوم قواعد البيانات السائدة قبل انتشار الشبكات التي كان مفهوما أنها مخزنة داخل النظام أو تنقل علي واسطة مادية تحتويها. ومادة أو محتوى موقع الإنترنت من نصوص ورسوم وأصوات ومؤثرات حركية (يطلق علي المؤثرات الصوتية والحركية لوسائط المتعددة - Multimedia) ونحن نري أن المصنف الرقمي يشمل كافة المصنفات المتقدمة، فبرنامج الكمبيوتر من حيث البناء والأداء مصنف رقمي، وقاعدة البيانات من حيث آلية ترتيبها وتبويبها والأوامر التي تتحكم بذلك تنتمي إلي البيئة الرقمية، وذات القول يرد بالنسبة لكافة العناصر المتقدمة، وبالتالي نري أن أي مصنف إبداعى عقلي ينتمي إلي بيئة تقنية المعلومات يعد مصنفا رقميا وفق المفهوم المستطور للأداء التقني وفق اتجاهات تطور التقنية في المستقبل القريب، وهذا لا يؤثر علي انتماء المصنف بذاته إلي فرع أو آخر من فروع الملكية الفكرية، ونقصد هنا أن أسماء النطاقات مثلا ينظر لها كأحد المسائل المتعين إخضاعها لنظام الأسماء والعلامات التجارية بسبب ما أثارته من منازعات جراء تشابهها بالعلامات والأسماء التجارية وتطابقها في حالات عديدة أو لقيامها بذات المهمة تقريبا في البيئة الرقمية، والبرمجيات وقواعد المعلومات حسم الجدل بشأنها بأن اعتبرت مصنفات أدبية تحمي بموجب قوانين حق المؤلف- مع وجود اتجاه حديث وتحديدا في أمريكا وأوروبا يعيد طرح نجاعة حمايتها عبر آلية حماية براءات الاختراع- وسيثير محتوى موقع الإنترنت جدلا واسعا، فهل تحمل محتوياته كحزمة واحدة ضمن مفهوم قانون حق المؤلف، أم يجري تفصيل هذه العناصر ليسند اسم الموقع إلي الأسماء التجارية وشعار الموقع إلي العلامات التجارية- كعلامة خدمة مثلا- والنصوص والموسيقى والرسوم إلي قانون حق المؤلف كمصنفات أدبية.

## تحديد المصنفات الرقمية:

من الوجهة التاريخية ابتداء التفكير بحماية أجهزة الكمبيوتر والاتصالات (المادية) بوصفها معدات ووسائل تقنية المعلومات، فكان نظام براءات الاختراع هو النظام المتناسب مع هذا الغرض باعتبار براءة الاختراع ترد بشأن مخترع جديد يتصف بالإبتكارية والجدة وبالقابلية للاستغلال الصناعي. ويتمثل المصنفات الرقمية ببرامج الحاسوب (الكمبيوتر) وبقواعد البيانات وبالدوائر المتكاملة، أما في بيئة الإنترنت فتتمثل بأسماء نطاقات أو مواقع الإنترنت، وبمحتوى المواقع من مواد النشر الإلكتروني نصوصا وصورا ومواد سمعية ومرئية (الوسائط المتعددة).

## برامج الحاسوب:

تعد برامج الحاسوب أول وأهم مصنفات المعلوماتية أو تقنية المعلومات التي حظيت باهتمام كبير من حيث وجوب الاعتراف بها وتوفير الحماية القانونية لها، والبرمجيات هي الكيان المعنوي لنظام الكمبيوتر دونها لا يكون ثمة أي فائدة للمكونات المادية من الأجهزة والوسائط وهي بوجه عام تنقسم من الزاوية التقنية إلى برمجيات التشغيل المناط بها إتاحة عمل مكونات النظام معا وتوفير بيئة عمل البرمجيات التطبيقية، وتمثل البرمجيات التطبيقية النوع الثاني من أنواع البرمجيات وهي التي تقوم بمهام محددة كبرمجيات معالجة النصوص أو الجداول الحسابية أو الرسم أو غيرها، وقد تطور هذا التقسيم للبرمجيات باتجاه إيجاد برمجيات تطبيق ثابتة وأنواع مخصوصة من البرمجيات تزوج في مهامها بين التشغيل والتطبيق، هذا من ناحية تقنية مبسطة جري إيضاحه تفصيلا في القسم الأول من هذا الكتاب، أما من ناحية الدراسات والتشريعات القانونية فقد أثر فيها عدد من المفاهيم المتصلة بأنواع

البرمجيات، أبرزها برمجيات المصدر وبرمجيات الآلة والخوارزميات ولغات البرمجة وبرامج الترجمة، ونعرض فيما يلي بإيجاز لهذه المفاهيم:

١- برنامج المصدر: هي الأوامر التي يضعها المبرمج أو مؤلف البرنامج وتكون مدركة له لكنها غير مدركة للآلة التي هي الكمبيوتر كجهاز مادي (وحدة المعالجة تحديداً) ويستخدم في تأليفها أو وضعها لغات البرمجة التي شهدت تطوراً مذهلاً عبر السنوات الخمسين المنصرمة، هذه اللغات التي تختلف من حيث سهولتها وتعقيدها ومن حيث فاعليتها في إنجاز البرنامج للغرض المخصص له.

٢- برنامج الآلة: وهو عكس مفهوم برنامج المصدر تماماً، إذ تتركه الآلة وتستطيع التعامل معه وتشغيله، وبين برنامجي المصدر والآلة توجد برامج ذات غرض تحويلي (أو برامج ترجمة) بموجبها تتحول برامج المصدر إلى برامج آلة.

الخوارزميات: العناصر والرموز الرياضية التي يتكون منها بناء البرنامج وهي كالأفكار والحقائق العلمي ليست محل حماية لأنها ليست موضعاً للاستثمار (مادة ٢/٩ من اتفاقية ترينس) لكنها متى ما نظمت على شكل أوامر ابتكارية لتحقيق غرض معين أصبحنا أمام برنامج، وهو بهذا الوصف أن توفرت له عناصر الجدة والابتكار والأصالة محل للحماية شأنه شأن أي من مصنفات الملكية الفكرية الأدبية الأخرى.

وقد أثارت برامج الحاسوب جدلاً واسعاً في مطلع السبعينات بشأن طبيعتها وموضع حمايتها من بين تشريعات الملكية الفكرية، وترددت الآراء بين من يدعو لحمايتها عبر نظام براءات الاختراع لما تتطوي عليه من سمة الاستغلال الصناعي واتصالها العضوي بمنتج مادي صناعي، وبين من ذهب إلى حمايته عبر نظام الأسرار التجارية إذ تتطوي في الغالب على سر تجاري يتجلى

بالأفكار التي انبني عليها أو الغرض من ابتكارها، وبين داع إلي حمايتها عن طريق الشروط العقدية التي تجد مكانها في رخص الاستخدام أو اتفاقيات الاستغلال. لكن كافة هذه الآراء لم تصمد أمام الرأي الذي وجد في البرمجيات عملاً ابتكارياً أدبياً، يضعها ضمن نطاق مصنفات الملكية الأدبية (حق المؤلف) إذ هي أفكار وترتيب لخوارزميات تفرغ ضمن شكل ابتكاري إبداعي، وسماتها وصفاتها المميزة تتقابل مع عناصر الحماية لمصنفات الملكية الأدبية، وبالرغم من استمرار وجود نظم قانونية توفر الحماية للبرمجيات عبر واحد أو أكثر من الآليات المتقدم الإشارة إليها إلا أن الاتجاه التشريعي الغالب اعتبرها أعمالاً أدبية وحماها بموجب تشريعات حق المؤلف.

ووفق اتفاقية تريبس فإن البرمجيات محل للحماية سواء أكانت بلغة الآلة أم المصدر (م ١٠/١) ولمؤلفها كافة الحقوق المالية والمعنوية لمصنفات حق المؤلف إضافة إلي حقه في إجازة أو منع تأجيرها. شأنها شأن التسجيلات الصوتية والمرئية (م ١١)، ويستتقي وفق هذه المادة حالة التأجير التي لا يكون فيها البرنامج الموضوع الأساسي للتأجير، وأما بخصوص مدة الحماية فإنها تمتد إلي ٥٠ عاماً محسوبة علي أساس حياة الشخص الطبيعي فإن لم تكن كذلك فمن نهاية السنة التي أجز فيها النشر أو تم فيها إنتاج العمل (م ١٢ تريبس).

#### ١-٢-٢ قواعد البيانات Database

قواعد البيانات هي تجميع مميز للبيانات يتوافر فيه عنصر الابتكار أو الترتيب أو التوزيع عبر مجهود شخصي بأي لغة أو رمز ويكون مخزناً بواسطة الحاسوب ويمكن استرجاعه بواسطتها أيضاً. ومناطق حماية قواعد البيانات - بوجه عام - هو الابتكار كما عبرت عنه الاتفاقات الدولية في هذا الحقل، فالمادة ١٠/٢ من اتفاقية تريبس نصت على

أنه:- تتمتع بالحماية البيانات المجمعة أو المواد الأخرى سواء كانت في شكل مقروء آليا أو أى شكل آخر إذا كانت تشكل خلقا فكريا نتيجة انتقاء وترتيب محتواها، كما نصت المادة ٥ من الاتفاقية العالمية للملكية الفكرية لسنة ١٩٩٦- غير نافذة - على أنه:- تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر ابتكارات فكرية بسبب محتواها أو ترتيبها. لكن لا تجرى كافة النظم القانونية والقوانين على هذا النهج، فالتوجيهات الصادرة عن الاتحاد الأوروبي في ١١/٣/١٩٩٦ والقانون الفرنسي الصادر في عام ١٩٩٨ لا يشترطان شرط الابتكار لحماية قواعد البيانات، بل يكفي ما بذل من جهد مالي أو بشري أو مادي وما أنفق من أجل إعداد قاعدة البيانات وسندا لذلك فإن القانون الفرنسي المشار إليه يحمي قواعد البيانات لمدة خمس عشرة سنة ويحظر أى إعادة استعمال سواء لجزء أو لمادة كلية من قاعدة البيانات عن طريق توزيع نسخ أو الإيجار أو النقل على الخط ويحظر النقل الكلي أو الجزئي - الجوهري - من محتوى قاعدة البيانات بأى شكل، متى كان الحصول أو تقديم هذا المحتوى قد استلزم استثمارات جهرية كما وكيفا، وسواء أكان النقل دائما أم مؤقتا على دعامة بأى وسيلة أو تحت أى شكل.

والابتكار يستمد أما من طبيعة البيانات نفسها وإما من طريق ترتيبها أو إخراجها أو تجميعها أو استرجاعها، ومحتوى البيانات في حد ذاته لا يعتبر عملا ابتكاريا، ومن هنا فإن الابتكار لا يتحقق إلا إذا عكست قاعدة البيانات سمات شخصية لواضعها، وقد قضت محكمة (نانت) التجارية الفرنسية في عام ١٩٩٨ بأن الابتكار الذى يتعلق بقاعدة البيانات على الانترنت يقتضي توافر جهد جاد فى البحث والاختيار والتحليل والذى عندما يقارن بمجرد التوثيق تظهر أهمية الجهد المبكر للعمل (مشار إلى هذا القرار فى مؤلف جينشار وآخرين، الانترنت والقانون، منشورات مون كريستان، ١٩٩٩

باريس، ص ١٩٢) أما قضاء محكمة النقض المصرية فإنه يتوسع فى مفهوم الابتكار، فقد قضت محكمة النقض المصرية فإنه يتوسع فى مفهوم الابتكار، فقد قضت محكمة النقض المصرية عام ١٩٦٤ بأن فهرسة إحدى كتب الأحاديث النبوية يعد عملاً ابتكارياً لأنه يكفي أن يكون عمل واضعه حديثاً فى نوعه ويتميز بطابع شخصي خاص وأنه يعتبر من قبيل الابتكار فى الترتيب أو التنسيق أو بأى مجهود آخر أن يتسم بالطابع الشخصي. (نقض مدنى فى ٧ يوليو ١٩٦٤- مجموعة النقض المدنى المصرى سنة ١٩٦٤، ص ٩٢٠).

وعليه، فإن البيانات أو المعلومات المخزنة فى نظم الحواسيب (بشكل مجرد) ليست محل حماية، كما بالنسبة للقوانين والأنظمة وقرارات القضاء مثلاً، لكنها متى ما افرغت ضمن قاعدة بيانات وفق تصنيف معين وبآلية استرجاع معين ومتى ما خضعت لعملية معالجة تنتج ذلك فإنها تتحول من مجرد بيانات إلى قاعدة معطيات، وينطوى إنجازها بهذا الوصف على جهد ابتكارى وإبداعي يستوجب الحماية، وبتزايد أهمية المعلومات، ولما حققته بنوك المعلومات من أهمية قصوى فى الأعمال والنشاط الإنسانى بوصفها أمست ذات قيمة مالية كبيرة بما تمثله، وباعتماد المشروعات عليها، ولتحول المعلومة إلى محدد استراتيجى لرأس المال، بل أن البعض يراه مرتكزاً لا محددات فقط، نشط الاتجاه التشريعى فى العديد من الدول لتوفير الحماية القانونية لقواعد البيانات (أنظر جدول ١).

والاعتراف لقواعد البيانات بالحماية جاء وليد جهد واسع لمنظمة الوايبو ولمجلس أوروبا الذى وضع عام ١٩٩٦ قواعد إرشادية وقراراً يقضى بالنص على حماية قواعد البيانات ضمن قوانين حق المؤلف.

## طوبوغرافيا الدوائر المتكاملة circuits Topographies of integrated

مثلت شبكة الموصلات فتحة جديدا ومميزا في حقل صناعة الإلكترونيات وتطوير وظائف التقنية العالية اعتبارا من منتصف القرن المنصرم، ومع تطور عمليات دمج الدارات الإلكترونية على الشريحة للقيام بمهام ووظائف إلكترونية أصبح التميز والخلق الإبداعي يتمثل آليات ترتيب وتنظيم الدوائر المدمجة على شريحة شبه الموصل، بمعنى أن طوبوغرافيا الشريحة انطوى على جهد إبداعي مكن من تطوير أداء نظم الحواسيب بشكل متسارع وهائل وبالاغتماد على مشروع قانون الحماية التي أعدته اللجنة الأوروبية أصدر مجلس أوروبا عام ١٩٨٦ دليلا لحماية الدوائر المتكاملة بغرض توفير الانسجام التشريعي بين دول أوروبا بهذا الخصوص، وفي عام ١٩٨٩ أبرمت الاتفاقية واشنطن بشأن الدوائر المتكاملة ( أى المنتجات التي يكون غرضها أداء وظيفة إلكترونية) ووفقا لاحصاء ١٩٩٩ فإن عدد الدول الموقعة على هذه الاتفاقية ٨ دول ليس من بينها سوى دولة عربية واحدة هي مصر، ولم تدخل هذه الاتفاقية حيز التنفيذ بعد، لكن تنظيم اتفاقية ترنس لقواعد حماية الدوائر المتكاملة ( المواد ٣٥ - ٣٨) ساهم في تزايد الجهد التشريعي في هذا الحقل باعتبار أن من متطلبات العضوية إنفاذ موجبات اتفاقية ترنس التي من بينها اتخاذ التدابير التشريعية المنفقة مع قواعدها ومن بينها طبعاً قواعد حماية الدوائر المتكاملة.

### المخاطر الأمنية للإنترنت:

#### - التجسس الإلكتروني:

وذلك بالاعتداء على سرية المعلومات الموجودة على الحاسب دون إذن صاحبها ودون معرفة بالاستعانة بالأقمار الصناعية وتستخدم الولايات المتحدة تلك التقنية في معرفة المعلومات ثم تحليلها.



#### - القرصنة:

وهي الاستخدام أو النسخ غير المشروع لنظم التشغيل، ولبرامج الحاسب وذلك بهدف بيعها بمقابل مادي زهيد الأمر الذي يضر بمنتجاتها.

#### - الإرهاب الإلكتروني:

وهو هجوم علي نظم المعلومات التي تملكها الدولة الإلكترونية أو الحكومة الإلكترونية بهدف شل حركتها الإدارية والعسكرية.

#### - الجريمة المنظمة:

وهي تلك الجريمة التي يستخدم الجناة فيها أرقى وسائل التقنية الحديثة في ارتكاب جرائمهم وذلك بإدارة تنفيذ تلك الجريمة عن طريق شبكة الإنترنت. وتحترف تلك الجريمة المنظمة جماعات المافيا التي استفادت من التكنولوجيا والعولمة والتي منحت تلك الجريمة بفصل تلك التقنية التي لا تعرف حدود جغرافية انتشار واسع المدى.

#### - المواقع المشبوهة:

وهي التي تنسخ وتردد أخبار غير صحيحة ومعادية وتلفق الأخبار وتقوم أيضا بإغراق البريد الإلكتروني وهذه المواقع المشبوهة قد تكون هدفها زعزعة نظام سياسي ما أو الفتك بمعتقدات دينية أو عادات أخلاقية- أو بالقذف والسب وتشويه سمعة الآخرين:

وفيها يتم مهاجمة أشخاص معينة وذلك بسرد قصة حياتهم وتلفيق أحداث معينة بهدف هدم سمعتهم الشخصية في نظر المجتمع التي تنتمي إليه. أو الحصول علي صورة عادية لفتاة أو امرأة محترمة ثم تركيبها علي صورة امرأة أخرى عارية وإعادة بثها باعتباره تدعو للغير لممارسة الجنس معها.

#### - المواقع الإباحية:

وهي تقوم بنشر الصور والأفلام الإباحية بكل أنواعها وأشكالها حتى ترضي جميع الأعمال وتخطب الغريزة بتلك الأفلام الخليعة والتي من الممكن بثها من أي مكان بعد أن سقطت الحدود الجغرافية.

تلك المواقع تقدم للمشاهد علي شبكة الإنترنت الدعارة في سهولة وذلك بالتعاقد علي شبكة الإنترنت ومخاطبة الطرف الآخر علي الشبكة أي أن تلك الشبكة تقوم بدور القوادة في صورة تتناسب مع الواقع العالمي، ويستطيع أيضا المشاهد شراء الأفلام الخليعة لرؤيتها علي شاشة الكمبيوتر، أو شاشة الهاتف.

الأمر الذي يؤدي إلي انتشار الإباحية وانهيار الأخلاق ولا سيما في المجتمعات المتعطشة إلي الحرية بكل صورها الأمر الذي يعد وابل علي تلك المجتمعات التي بدون مقدمات انتقلت من التحفظات الخلقي التام إلي الإباحية السامة دون مقدمات الأمر الذي يجعل هذا الأمر وبجد خطير علي تلك المجتمعات المتحفظة والشرقية بصفة خاصة.

وقد أثبت الإحصاءيات أن عدد زوار المواقع الإباحية لا تقل عن ٤,٧ مليون زائر في الأسبوع الواحد طبقا لإحصاء ماضي فما بالك اليوم.

علاوة علي ما تقدم فقد انتشرت الآن ظاهرة إيمان المواقع الإباحية التي بدعت تظهر علي الأطفال الذين يشاهدون الجنس في سن مبكرة علاوة علي العنف الجنسي.

#### - تزوير البيانات والمعلومات:

وذلك بالدخول إلي قاعدة البيانات وتعديل تلك البيانات مثل تغيير ملكية الأشياء أو تغيير اسم شخص أو تغيير رقم تليفون أو أي قاعدة بيانات لأي جهة هامة تساعد الجاني في ارتكاب جريمة ما.

ومن ذلك أيضا السطو علي بيانات بطاقة الائتمان بهدف الإستيلاء علي النقود من جهاز الصرف الآلي وذلك عن طريق كسر حماية البيانات الموجودة علي بطاقة الائتمان.

#### - القمار عبر الإنترنت:

يوجد علي شبكة الإنترنت الآن أكثر من ألف موقع ينفق فيه الأمريكيون فقط فيه ما يزيد علي مليار دولار.

#### - تجارة المخدرات والمواد المؤثرة علي العقل:

بات الأمر لا يقبله عقل فقد أصبحت الآن هناك مواقع تروج للمخدرات بل وصل الأمر إلي أن تلك المواقع تبين طريقة زراعة وصناعة المخدرات وكيفية تسويقها وقد يأخذ هذا صورة إعلامية ولكنه يهدف إلي الترويج وليس إلي الإعلام الهادف البناء.

#### - من مخاطر الجرائم الإلكترونية تهديد التجارة الإلكترونية الوليدة:

وذلك عن طريق محاولة البعض فك شفرات التعاقد والتعرف علي معلومات متعلقة بالصفقات والترقيات الإلكترونية من تلك أمثلة الحرب الضروس في الولايات المتحدة التي استحدثت أخير واكتشافها مكتب الشكاوي لبحث تلك الجرائم التابع للمباحث الفيدرالية بالولايات المتحدة، وكذلك تواجه بعض الدول الأوروبية والآسيوية تلك المشكلة وأن كانت بحجم أقل من ذلك.

ويزيد الأمر تعقيد عدم معرفة أطراف التعاقد الإلكتروني ببعضهم ببعض علاوة علي أن تلك المواقع حينما تبرز لها رقم البطاقة الائتمانية والشفرة المتعلقة بها وتكون تلك المواقع مشبوهة فأنت لا تأمن علي نفسك من إعادة استعمالها دون معرفة بذلك.

- جرائم ذوي الياقات البيضاء:

تلك الجرائم التي يرتكبها مجرمون ذات طبيعة خاصة وهم الفئة التي لديها من الخبرات والمعرفة بالتقنية الكثير ولا سيما في جرائم الرشوة والاستيلاء على الأموال وتزوير البيانات والمستندات وتزوير الأوراق المالية والتلاعب بأسواق البورصة.

- من مخاطر الجرائم الإلكترونية أنها تنتهك الخصوصية:

وذلك عن طريق التسلل ومعرفة بيانات مستخدمي شبكة الإنترنت دون علمهم والإطلاع على كافة ما يحتويه جهاز الكمبيوتر من بيانات وتخص صاحبة الأمر الذي يستغله البعض في جرائم الابتزاز.

١٥- من مخاطر استعمال تقنية الكمبيوتر والإنترنت محاولة البعض انتحال صفة آخرين والتعامل باسمهم وصفقتها. وذلك في النصب على الغير.

- الإغراق بالرسائل:

وذلك بإرسال آلاف الرسائل إلى البريد الإلكتروني لمستخدمي شبكة الإنترنت على البريد الخاص بهم الأمر الذي يخرب هذا البريد بل وينقل هذا الفيروس إلى البريد الإلكتروني لمستخدم آخر بطريق العدوى الأمر الذي يهدد بوقف التعامل على شبكة الإنترنت الأمر الذي يؤدي إلى انقطاع الخدمة ووقف بثها.

- الاقتحام والتسلل:

إلى أجهزة الحاسب المتعلقة بأماكن أمنية تتعلق بالجيش أو بالبوليس أو بالبنوك بهدف تغيير بياناتها أو تدميرها أو الحصول على بيانات متعلقة بها لاستخدامها في أغراض إجرامية واستطاعت المباحث الفيدرالية FIB اعتراض العديد من تلك المحاولات.

## **الفصل الأول**

**فيروسات الحاسبات**

**أنواعها وأشكالها**

**وكيفية مواجهتها**



## أمور تتعلق بالإنترنت:

الإنترنت عبارة عن بحر مفتوح من عمليات الكمبيوتر وعلي ذلك فهي معرضة للكثير من المخاطر المتعلقة بسرية المعلومات لذلك فبمجرد اتصالك بالإنترنت فأنت معرض لعملية الاختراق وسرقة البيانات وبما أن الإنترنت ليس لها مالك أو حاكم حتى هذه اللحظة وتدير نفسها تلقائياً (أو بالأحرى نحن المستخدمين الذين نديرها)، فيجب أن نعلم أنه إذا لم نستطيع نحن سكان عالم الإنترنت أن تحكمها بعقلانية فسيأتي اليوم الذي تتدخل الجهات الحكومية لإدارتها!

## مخاطر الإنترنت المحتملة<sup>(1)</sup>:

### \* سرقة المعلومات:

- ١- اعتراض رسائل البريد الإلكتروني.
- ٢- اختراق أجهزة الغير والإطلاع على المعلومات الموجودة فيها أو تغييرها.
- ٣- سرقة أرقام بطاقات الائتمان والأرقام السرية الأخرى.

### \* تعطيل نظام التشغيل:

- ١- إرسال فيروسات تتسبب في أعطال أيا كانت.
- ٢- مسح نظام التشغيل أو حذف ملفات نظام.

### \* وجود مواقع غير مناسبة:

- ١- مواقع إباحية.
- ٢- مواقع مافية للدين.

---

(1) [http // encyclonedia. Aarabiah. Net/ internet- Technology- software.](http://encyclonedia.Aarabiah.Net/internet-Technology-software)

أعداء الإنترنت:

• المتطفلون Hackers:

المتطفل هو الشخص الذي يشعر بالفخر لمعرفته بأساليب عمل النظام أو الشبكات حيث يسعى للدخول عليها بدون تصريح، وهؤلاء الأشخاص عادة لا يتسببون بأي أضرار مادية.

• المخربون Crackers:

المخرب هو الشخص الذي يحاول الدخول علي أنظمة الكمبيوتر دون تصريح، وهؤلاء الأشخاص عادة ما يتسببون في أضرار مادية بعكس المتطفلين.

• الفيروسات Viruses:

الفيروس هو برنامج يكرر نفسه علي نظام الكمبيوتر عن طريق دمج نفسه في البرامج الأخر، وكما أن الفيروسات خطيرة للإنسان لدرجة أنها قد تقضي عليه، فالفيروسات التي نتحدث عنها قد تقضي علي الكمبيوتر، وقد تأتي في مختلف الأشكال والأحجام بل أن بعضها لا يسمى فيروسا مثل الدود Worms وأحصته طروادة Trojan Horses وبعض الفيروسات ليست خطيرة وإنما مزعجة، بعض التصرفات التي قد تجلب الفيروسات.

١- تشغيل البرامج من الإنترنت دون فحصها والتأكد من سلامتها.

٢- تشغيل البرامج من أقراص دون فحصها والتأكد من سلامتها.

٣- عدم وضع نسخ احتياطية للمعلومات المهمة.

٤- عدم وجود مضاد جيد للفيروسات أو عدم وجود نسخة منه. الحماية من الفيروسات يجب أن لا تبالغ في إجراءات الحماية ضد



الفيروسات، كما يجب ألا تتهاون فيها، بحيث لا إفراط ولا تفريط الأمر المهم أن يكون لديك برنامج مضاد فيروسات ممتاز كبرنامج Norton Antivirus 5.0 وتأكد من تحديثه بصورة دورية عن موقع الشركة المنتجة [www. Norton. Com](http://www.Norton.Com) اعتبر - من باب الحماية- أن جميع البرامج التي تنزلها من الإنترنت أو من الأقراص ملغومة بالفيروسات ولذلك قم بفحصها قبل تشغيلها وأعلم أن النظام الوحيد الآمن ١٠٠% هو المكتوب باليد أو المحفوظ في الذاكرة واحتفظ دائما بنسخ بديلة للمعلومات المهمة.. وضع في ذهنك أن الوقاية خير من قنطار علاج.

#### \* المحاكاة: Spoofing

المحاكاة هو مصطلح يطلق علي عملية انتحال شخصية للدخول إلي النظام. حزم الـ IP تحتوي علي عناوين للمرسل والمرسل إليه وهذه العناوين ينظر إليها علي أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة، ومن خلال طريقة تعرف بمسارات المصدر Source Routing فإن حزم الـ IP قد يتم إعطائها شكلا تبدو معه وكأنها قادمة من كمبيوتر معين بينما هي في الحقيقة ليست قادمة منه، وعلي ذلك فإن النظام إذا وثق ببساطة بالهوية التي يحملها عنوان مصدر الحزمة فإنه يكون بذلك قد حوكي (خدع). البريد الإلكتروني يمكن أيضا أن يخدع بسهولة ولكن النظام المؤمن بشكل جيد لا يثق بهذه المصادر ولا يسمح عموما بالحركة المسيرة من قبل المصدر Source routed.

بعض خيارات الحماية في الإنترنت:

- عدم الارتباط بالإنترنت.
- التوثيق Authentication.

- التشفير Encryption .

- جدران النار Ftirwalls

أسلوب "تقاطع المواقع" يتيح لقرصنة المعلوماتية إدخال شفرة تسلسل خاصة إلى الأجهزة الشخصية<sup>(١)</sup>:

هل تنتهك الإنترنت الحياة الخاصة للناس؟

هيئات مدافعة عن حماية المعطيات الشخصية والحياة الخاصة أعربت في تقارير لها، أن محرك البحث "غوغل" قد يكون بصدد انتهاك معايير حماية المعطيات الشخصية لمستخدميه عندما يحتفظ لأوقات طويلة بمواضيع بحثهم. وقالت "مجموعة الفصل ٢٩" الأوروبية التي تمثل عدة هيئات استشارية تقوم بتوفير النصائح والإرشادات للاتحاد الأوروبي حول ما يتعلق بسياسة حماية الحياة الخاصة في رسالة للهيئة المشرفة علي غوغل أن المدة التي يتم خلالها الاحتفاظ بمواضيع البحث تصل إلى سنتين في الكثير من الحياة وهو ما يطرح عدة أسئلة.

وقالت متحدة باسم غوغل أن انشغالات "مجموعة الفصل ٢٩" تتعلق أساسا بالمدة التي تستغرق بين ١٨ و ٢٤ شهرا وهو ما تعده زمنا طويلا جداً. وأثناء كل عملية بحث، يجمع المحرك غوغل أنواق المستخدمين وتوجهاتهم وأفكارهم واهتماماتهم وهي المعطيات التي يمكن استخدامها من قبل طرق ثالث (مثل الجماعات الدينية والإعلانية). وأضافت المتحدة أن غوغل. بمبادرة خاصة منه، قرر قبل مدة قصيرة، قصر مدة الاحتفاظ بتلك المواضيع علي سنتين فقط.

---

(1) http://www.Alqabas.Com.kw/Final/Newspaper Website/ Newspaper Public/ ArticlePage. Aspx...

غير أن صحيفة فايننشال تايمز أشارت إلى أن عدة خبراء يعتقدون أن هذه المدة طويلة جدا ويطلبون من غوغل تبرير سياسة الاحتفاظ بالمعطيات الخاصة.

#### ثغرة تفضح الزبائن:

وأعلنت شركة غوغل، أنها قامت بإصلاح عطل أمني رئيسي ساد خدماتها المقدمة إلى زبائنها وهدد بفحص ملفاتهم الشخصية بسهولة أمام قراصنة الإنترنت، وذلك بعد أسابيع من تلقيها تقارير عن وجود تلك الثغرة من شركة متخصصة في مجال أمن الشئون المعلوماتية.

وأكدت الشركة أنها لا تمتلك أي دليل على حدوث خروقات لبرامجها المقدمة إلى الأجهزة الشخصية خلال هذه الفترة، رغم أن الثغرة وجدت في ٨٠ بالمائة من الحالات المسجلة.

وكانت شركة واتش فاير، المعنية بشئون الأمن المعلوماتي، قد كشفت وجود هذه الثغرة أخيرا، وقد أكد داني ألن، وهو أحد خبراء الشركة على أهمية الكشف قائلا " الأمر شديد الأهمية، نظرا لحساسية المهمة التي تؤديها خدمات غوغل لزبائنهم على أجهزتهم الشخصية".

يذكر أن الميزات التي يقدمها هذا البرنامج الخاص لغوغل، على الصفحة الخارجية لأجهزة الكمبيوتر الشخصية، تتضمن تسهيل تقنيات البحث عن الملفات، والبريد الإلكتروني، والرسائل الفورية، وقد بدأ العمل به بشكل مجاني منذ عام ٢٠٠٤.

وكانت الثغرة التي اكتشفتها الشركة الأمنية متمثلة في مرحلة تشغيل البرنامج الأولية، والتي كانت عرضة للخرق بأسلوب "تقاطع المواقع" الذي يتيح لقراصنة المعلوماتية إدخال شيفرة تسلل خاصة إلى الأجهزة الشخصية.

وتتيح تلك الشيفرة، التي لا يمكن رصدها ببرنامج مكافحة التسلل العادية، للقرصان تصفح المعلومات التي يرغب بها علي الأجهزة الشخصية لضحاياه، أو التحكم بشكل كلي بالجهاز.

وقالت شركة واتش فاير أنها رصدت الثغرة وأبلغت غوغل بوجودها فوراً، وأن تلك الأخيرة بادرت إلي إخطارها بالمقابل بأنها أصلحت هذا الخلل، وطمأنت الشركة كل مستخدمي النظم إلي أن التعديلات سيتم تنزيلها إلي البرنامج بشكل تلقائي، داعية إياهم إلي عدم اتخاذ أي خطوات احتياطية خاصة. غير أن خبراء أمن الشبكة العنكبوتية لدى واتش فاير، حذروا من إمكان بروز خلل جديد في الفترة المقبلة، يقوم علي استغلال القرصنة لطبيعة عمل البرنامج، للاحية ربطه بين الأجهزة الشخصية وموقع البحث.

لكن هذا التحذير قابله تطمين من غوغل، التي أكدت في رسالة إلكترونية أنها "أخذت العديد من الخطوات لحماية عملاتها والتصدي لهذه الهجمات". وكشفت الرسالة أن الشركة "أضافت طبقة جديدة من اختبارات الأمان، للتصدي للمخاطر التي أثارها واتش فاير وسواها"، لكت هذا الرد لم يكن كافياً لطمأنة خبراء الأمن، الذين دعوا إلي تطوير وسائل لمقاومة القرصنة الإلكترونية بشكل يواكب التقدم الكبير الذي تشهده تقنيات المعلوماتية.

تكتسب شبكة الإنترنت عامة، وGoogle خاصة، حجماً متزايداً في الحياة العملية والاقتصادية للكثير من الناس، غير أنها تحولت أيضاً إلي "كتاب مفتوح" يكشف أدق التفاصيل عن حياة الناس الاجتماعية، حتى تلك التي يحاولون إخفاءها أثناء رحلة البحث عن شريك الحياة.

فقد أظهرت الدراسات أن أعداداً متزايدة من الناس يعتمدون إلي استخدام محرك غوغل لسير أغوار الطباع الحقيقية لشركائهم العاطفين، خاصة الجوانب التي يحرصون علي إخفاءها.

وفي هذا السياق قالت كاتيا ليرد التي تصنف نفسها "مغربة بالتواصل الاجتماعي الإلكتروني" بأنها تحرص دائما علي توجيه صديقاتها نحو استخدام قدرات موقع غوغل لمعرفة تفاصيل عن شركائهن، وتحرص ليرد علي تحضير صديقاتها لأي نتائج قد يظهرها البحث بحيث لا يقعن تحت هول الصدمة.

وتروي الشابة التي لا تتجاوز من العمر ٢٤ عاما تفاصيل من تجربتها قائلة: "وفي بعض الأحيان، قد تكون النتائج مرعبة... ذات مرة قادني البحث عن معلومات حول أحد الشبان الذي أراد الخروج معي إلي اكتشاف أنه مفتون بمصاصي الدماء".

وشرحت ليرد أهمية ما تفعله قائلة: "لا يمكنك الحصول علي هذه التفاصيل حول الشاب من خلال بضع جلسات معه في المقهى".

كما كشفت شابة أخرى أنها كانت تستعد للخروج في موعد مذبذب مسبقاً، مع شاب رشحته لها أمها باعتباره "الشخص المناسب" قبل أن تكتشف صورة عاريا في مغطس السباحة علي موقع Myspace.

فيما وقعت ليزا فيليبس ضحية تشابه الأسماء، عندما قامت بالبحث عن معلومات حول اسمها عبر شبكة الإنترنت، لتكتشف وجود صور عارية لممثلة أفلام خليعة تحمل الاسم نفسه.

من جهته أشاد براد وايت إلي أهمية المعلومات التي يقدمها موقع غوغل، بطريقة غير مباشرة طبعاً، عن طباع الأشخاص وأهوائهم، لافتاً إلي أنه ارتبط بصديقته الحالية بعد ما اكتشف نوعية الأغاني التي تحب الاستماع إليها عبر الشبكة.

إلا أن آخرين أشاروا إلي الميزة الأهم التي يكفل موقع البحث تحقيقها لسرواده، وهي كسر جليد اللقاء الأول، رغم أن طرفي اللقاء لن يقرأاً بأنهما أجريا بحثاً خاصاً عبره.

وأوضح ليفيد سيلفر، الأستاذ المساعد في دراسات الإعلام بجامعة سان فرانسيسكو ذلك: "سجل الواحد منهم قبالة الآخر وبهرز رأسه بلهفة عند سماع أي قصة، رغم معرفته المسبقة بكامل تفاصيلها". وفي نهاية المطاف ينصح المهتمون بالجانب الاجتماعي من العلاقات بالنظر إلى المعلومات التي تقدمها مواقع البحث بصورة موضوعية، ويمنح "اللقاء الأول" والاحتكاك الإنساني المباشر فرصة النجاح.

#### قضايا وإيقاع بمستخدمين:

شركة مايكروسوفت العملاقة للبرمجيات كانت قد رفعت دعاوى قضائية ضد ١١٧ موقعا علي الإنترنت حاولت الإيقاع بالمستخدمين للشبكة الدولية وخذاعهم باسترجاعهم لتقديم معلومات شخصية وبيانات تتعلق بحساباتهم وبطاقاتهم الائتمانية.

وقال أرون كورنيلوم محامي الشركة أن الشرطة رفعت هذه الدعاوى أمام محكمة اتحادية في سياتل علي أشخاص لم يسمهم وطلبات السماح لها بالحصول علي معلومات عن القائمين علي تشغيل تلك المواقع ومتابعة بريدّها الإلكتروني.

وتبرز هذه الدعاوى القضائية القلق المتزايد من المواقع التي يشغلها محتالون علي الإنترنت يرسلون ملايين الرسائل الإلكترونية يوميا ويزعمون فيها أنهم ينتمون إلي بنوك معتمدة أو شركات ومؤسسات مماثلة.

وترشد هذه الرسائل الإلكترونية الأشخاص أو الجهات التي تتلقاها إلي مواقع علي شبكة الإنترنت لا يمكن تمييزها في أغلب الأحيان عن المواقع الأصلية الحقيقية للشركات وتطلب إليهم نكر بيانات شخصية ومعلومات عن بطاقت الائتمان.

ولا يستغرق الأمر سوى ثوان معدودة لوصول الرد من تلك المواقع التي تجني ملايين الدولارات من ضحاياها.

## جواسيس الإنترنت:

تفيد آخر التقارير أن عيوننا لا تتركز بالعين المجردة ترافق عمليات تصفح المواقع على الشبكة وتقوم الجهة المراقبة باستخدام ما أصبح يطلق عليه جواسيس الإنترنت، أو فيروسات شبكة الإنترنت، وهي رموز إلكترونية تختفي وراء صور لا يتعدى حجمها البيكسل الواحد، وهي وحدة لقياس حجم الصور الإلكترونية، من أجل جمع معلومات حول عادات المستخدمين في تصفح الإنترنت ومن الصعب جدا مقاومة هذا النوع من الفيروسات، ويقول المتخصصون في حماية حريات المستهلكين، أن الصور الخفية هي أول جيل مما يسمى ببرامج تجسس مصممة لمراقبة تحركات مستخدمي الإنترنت بدون علمهم، وتلجأ تلك المواقع عادة إلى استخدام صور غير مرئية ليضمّنوا من أن الصورة التي يريدون أن يجذبوا عيون المستخدم إليها موضوعة في المكان الصحيح.

ولكن بعض الشركات بدأت في وضع صور غير مرئية، حجمها بيكسل مربع واحد فقط، على صفحات يهدف منها أغراضا أخرى.

ويقول ديفيد باتيسار، من مركز أيبك لحماية المعلومات الشخصية، أنه توجد طريقة سرية لجميع معلومات عن الأشخاص، وذلك بوضع صور ألوانها متجانسة تماما مع ألوان الخلفية حتى تصبح غير مرئية بتاتا، ويشير إلى أن متصفح الشبكة لا يستطيع رؤية هذه الفيروسات، لكن الكمبيوتر يراها ويتعامل معها وكأنها صورة إلكترونية، ولهذا السبب تخفي رموز أنش تي أم إل، أو رموز لغة الكمبيوتر، وراء الصور غير المرئية، وتستعمل هذه الرموز لجمع معلومات عن عادات المتصفح، وعندما تزور موقع ما، يطلب برنامج التصفح كل مكونات الصفحة من صور، ونصوص وإطارات وإعلانات من عدة كمبيوترات ويذهب عادة طلب الصورة غير المرئية المحتوية على الفيروس إلى سيرفر مهمته جمع معلومات عن العديد من

مستخدمي الشبكة، وعندما يطلب متصفح مثل نيتسكيب كوميونيكيتز أو إنترنت إكسبلورر معلومات ما فهو يرسل أيضا معلومات عن الجهاز والشخص الذي يستخدمه. وتستطيع رموز لغة الكمبيوتر المخفية طلب معلومات إضافية عن هذا الجهاز أو ذاك وكذلك عن أسماء المواقع التي زارها الجهاز.

وأفضل طريقة لمنع فيروسات الرقابة هي علي المواقع التي تحتوي علي تصميمات وصور ولكن ذلك لا يعني التخلص من انتباه الفيروسات لأن أي برنامج يقرأ لغة اتش تي إم إل، مثل البريد الإلكتروني، وغرف المحادثة يمكن أن تدخل عبره الفيروسات. وتعتمد معظم الشركات الآن إلي ملء صفحاتها بمثل هذه الفيروسات، وإذا زرت صفحة كهذه فكل الصفحات الموجودة علي تلك الشبكة يمكنها جمع معلومات عنك.

وتتيح بعض المواقع مثل 'برايفسي نيت' معلومات عن جهازك ودرجة تعرضه للفيروسات وترسل المعلومات إلي شركات الإعلانات علي الإنترنت، مثل دويلكلبك وانكيك وتحقق لجنة تابعة لوزارة الصناعة الأمريكية في موضوع استخدام فيروسات الرقابة وقد أبدت قلقها من أن عملية الرقابة تتم بدون موافقة المستخدمين.

وقال باتسيار أنه في غياب حماية قانونية لا يستطيع الأشخاص العاديين فهم الموضوع ما لم يكن عندهم شهادة دكتوراه في برمجة الكمبيوتر. قاعدة بيانات لجرائم الإنترنت<sup>(1)</sup>:

طالب عدد من المؤسسات التجارية البريطانية الحكومة بإقامة قاعدة بيانات لمكافحة جرائم الإنترنت. وقال مسؤولو تلك المؤسسات الاستثمارية

---

(1) <http://www.Alqabas.Com.kw/Final/NewspaperWebsite/NewspaperPublic/ArticlePage.aspx...>



إن المطلوب هو إقامة مركز بريطاني علي غرار مركز شكاي جرائم الإنترنت الموجود في الولايات المتحدة، وتتركز مهمة المركز المقترح في تلقي الشكاوي وتحويلها إلي أجهزة التحقيق المختصة.

وطالبت المؤسسات الاستثمارية البريطانية أيضا بتوسيع القانون الصادر في عام ٩٠ والذي يحدد عقوبات إساءة استخدام أجهزة الكمبيوتر ليشمل أعمال التخريب عبر الإنترنت التي تؤدي لتعطيل نظم تكنولوجيا المعلومات. وقد جاءت تلك الدعوى عقب نشر نتائج إحصاء أجراه اتحاد الصناعات البريطاني، وأظهر أن جرائم الإنترنت تؤدي إلي إحجام الشركات، وخاصة الصغيرة منها التي يقل عدد موظفيها عن خمسمائة موظف، عن بيع السلع والخدمات عبر الإنترنت.

وقال ثلاثة وخمسون فقط من مجموع مسؤولي الشركات الذين استطلعت آراؤهم أنهم يعتبرون الإنترنت وسيطا مأمونا إجراء معاملات تجارية مع شركات أخرى، وأعرب إثنان وثلاثون بالمائة عن اعتقادهم بأن الإنترنت وسيلة آمنة لبيع السلع والخدمات.

كما أظهر الإحصاء أن مخربي الإنترنت ارتكبوا ٤٤,٨ بالمائة من أخطر جرائم الإنترنت التي تقع في العام، وأن موظفين سابقين نفذوا ١٢,٨ بالمائة من تلك الجرائم، في حين نفذت عصابات الجريمة المنظمة ١١,٥ بالمائة منها، وموظفو الشركات ٧,٩ بالمائة منها.

أما الشركات المنافسة فارتكبت ٥,٨ بالمائة من تلك الجرائم، وارتكبت جماعات مناهضة لسياسات معينة ٢,٦ بالمائة منها، والجماعات الإرهابية ١,٤ بالمائة منها. وأظهر الإحصاء أن الشركات العاملة في قطاع الخدمات المالية تخشي من الخسائر التي قد يلحقها بها مخربو الإنترنت، في حين

تتركز المخاوف في قطاعات أخرى علي الضرر الذي قد يلحق بسمعة الشركات وعلي خسارة ثقة عملائها وهي خسائر معنوية وليست مادية.

وذكر مسؤولو ٦٩ من الشركات التي شملها الإحصاء أن الخسائر المادية التي لحقت بهم بسبب جرائم الإنترنت كانت لا تذكر وظهر أن ٤ بالمائة فقط من مخاطر الجرائم كانت جرائم تتعلق ببطاقات الائتمان.

وأظهر الإحصاء أيضا أن ٤٠ بالمائة من الشركات لا تحتوي علي أقسام مختصة بمواجهة جرائم الإنترنت.

وقال ديجبي جونز مدير عام اتحاد الصناعات البريطانية أن نتائج الإحصاء تؤكد أن جرائم الإنترنت تعطل نمو الشركات. وذكر أن السبيل الوحيد لتجاوز تلك المشكلة هو تشديد الرقابة وتشديد قوانين مكافحة جرائم الإنترنت.

#### فيروس الحاسب والفيروس العضوي:

يشاع- خطأ- لدى البعض أن فيروس الحاسب هو فيروس عضوي طبيعي مثل بقية الفيروسات الطبيعية التي تخترق الكائنات الحية، وتتكاثر ذاتياً في داخلها، وتصيبها بالأمراض الفتاكة، والحقيقة أن فيروس الحاسب يحمل مجموعة من الخصائص التي يتميز بها الفيروس الطبيعي.

ما هي الصفات المشتركة بين الفيروس العضوي وفيروس الحاسب؟

١- يقوم الفيروس العضوي بتغيير الخصائص العضوية لخلايا الجسم، ويقوم فيروس الحاسب بتغيير وظائف البرامج الأخرى.

٢- يتكاثر الفيروس العضوي ويتسبب في إنشاء فيروسات جديدة، ويقوم فيروس الحاسب بإعادة إنشاء نفسه (Reproduce itself) فيظهر وكأنه يتكاثر ذاتياً.

٣- الخلية التي تصاب بفيروس العضوي لا تصاب بالفيروس نفسه مرة ثانية، وكذلك فيروس الحاسب الآلي، إذا أصاب برنامجا معيناً فلا يصيبه مرة أخرى.

٤- الجسم الذي ينقل إليه الفيروس الطبيعي العدوي قد يظل مدة طويلة دون ظهور أعراض المرض عليه، وكذلك البرامج المصابة بفيروس الحاسب قد تبقى مدة طويلة دون ظهور أعراض تخريبية عليها.

٥- في بعض الحالات يقوم الفيروس العضوي وفيروس الحاسب بتغيير شكلهما؛ حتى يصعب اكتشافهما والتغلب عليهما.

#### تعريف فيروس الحاسب<sup>(١)</sup>:

هو عبارة عن برنامج حاسب آلي مثل أي برنامج تطبيقي آخر، ولكن يتم تصميمه بواسطة أحد المخربين بهدف محدد، هو إحداث أكبر ضرر ممكن بنظام الحاسب الآلي، ولتنفيذ ذلك إعطاؤه القدرة علي ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتياً، مما يتيح له القدرة علي الانتشار بين برامج الحاسب المختلفة، وكذلك بين مواقع مختلفة في ذاكرة الحاسب حتى يحقق أهدافه التدميرية.

ولا يقتصر انتشار فيروس الحاسب الآلي علي النظام الذي يتواجد به، ولكنه ينتقل أيضا إلي نظم أخرى ذات صلة ببعضها. وقد تتحقق هذه الصلة من خلال قرصنة البرامج. كما تتحقق بدرجة أكثر انتشاراً من خلال وسائل الاتصالات، وهي الوسائل التي تؤدي إلي ربط عدد كبير من أجهزة الحاسب بشبكة تتحقق التواصل من خلالها، ومن ذلك يتضح إمكانية انتقال الآثار التخريبية لفيروس الحاسب من مدينة إلي أخرى أو من بلدة إلي أخرى أو من قسرة إلي قسرة وفي وقت قصير للغاية قد لا يتعدي الدقائق أو الثواني

---

(1) <http://www.B7b7.com/view-Art-440-.Html>

المعدودة، كما يتضح في الوقت نفسه مدى خطورة فيروس الحاسب، سواء على المستوى الفردي أم الجماعي، أم القومي، وسواء في وقت الحرب، أم السلم لما يحدثه من آثار تدميرية في أنظمة تشغيل الحاسبات الآلية، وهو ما ينتج عنه الكثير من الأضرار المادية والمعنوية التي تصيب برامج الحاسب والمعدات الإلكترونية ومستخدميها.

#### بعض نماذج الفيروسات:

فيروس "أحبك"، الذي خرج من الفلبين في ٤ مايو ٢٠٠٠ م ليس معقداً من الناحية الفنية مقارنة بفيروس "مليسا" Melisa الذي اجتاحت العالم العام الماضي، ولكنه أسرع منه بمراحل في الانتشار، وينتشر فيروس "أحبك" من خلال أنظمة الرسائل الفورية التي تتيح لمستخدمي الإنترنت التخاطب مباشرة مع بعضهم وبعض ويستهدف الفيروس أساساً أجهزة الكمبيوتر التي تعمل بنظام ويندوز الذي تنتجه شركة مايكروسوفت العملاقة وتلك التي تستخدم نظام "إكسبلورر" لتصفح الإنترنت ويظهر الفيروس في البريد الإلكتروني على صورة رسالة بعنوان "أحبك" I LOVE YOU وفي حالة فتحها ينتشر الفيروس في جميع العناوين المسجلة لدى مستخدمي البريد الإلكتروني في أجهزة الكمبيوتر الأخرى، ثم يتسلل إلى جهاز الكمبيوتر ليحرق محتوياته.

لقد كانت كارثة مفاعل "تشيرنوبيل" النووي الروسي في أوكرانيا في ٢٦ إبريل عام ١٩٨٦ هي الحافظ وراء برمجة فيروس سمي بنفس الاسم وينشط للعمل في نفس التاريخ من كل عام، ويؤكد الخبراء على أن فيروس تشرنوبيل بالغ الدقة ينتقل عبر شبكة الإنترنت؛ فيتسلل إلى أجهزة الكمبيوتر حيث يدمر المعلومات المخزنة، ويلغي الملفات الموجودة في الذاكرة، بل يضغط على القرص الصلب، مما يؤدي في حالات كثيرة إلى إتلاف تلك الرقائق وتدميرها، وكان هناك تحذيرات كثيرة منذ عام ١٩٩٨، وبطريقة بسيطة جداً.. أمكن تلافي أخطار الفيروس، وذلك بتغيير تاريخ نشاطه، ثم

إعادة تصويب التاريخ مرة أخرى بعد يوم أو يومين. وهذه الطريقة مأمونة في التعامل مع العديد من الفيروسات المؤقتة؛ مثل فيروس "مايكل أنجلو" الذي ينشط في ٢٦ مارس من كل عام لمسح معلومات القرص الصلب للأجهزة المصابة فيه كنكري مجنونة لميلاد فنان عصر النهضة "مايكل أنجلو"!!!.

أما فيروس حصان طروادة Trojan Horse فقد أخذ مبرمجه الفكرة اليونانية القديمة في إخفاء الجنود داخل الحصان الخشب...!!!

وهناك الآلاف من تلك الفيروسات برمجها عباقرة شياطين من البشر لا هم لهم غير الإيذاء، واستعراض القوة العلمية والدخول في ركاب التقدم العلمي من باب الشر ومن أجل فرض حلول علمية للقضاء علي الفيروس من جهتهم، لأنهم أعلم بما فعلوه من أسلوب علمي في صنع تلك الفيروسات.

#### فيروسات الحاسب في السلم والحرب:

ونظرا لأن القائمين بتطوير فيروسات الحاسب يقدمون كل يوم اختراعا جديدا في هذا المجال، وذلك بالتبعية للتطورات المتسارعة والمتلاحقة لتكنولوجيا عصر المعلومات.. فإنه لذلك قد يصبح فيروس الحاسب من أهم وأخطر أسلحة الحروب المستقبلية، وقد يكون استخدام فيروس الحاسب في الحروب علي هذا النحو أمرا مشروعاً- أي خارجا عن نطاق التجريم القانوني؛ حيث يباح في الحروب استخدام كافة الوسائل والأسلحة المساعدة علي تدمير قوات العدو وتدمير أسلحته، خصوصا إذا كانت أسلحة جديدة، لم يتم إدراجها في اتفاقيات دولية، كأسلحة محرمة دوليا.

أما في وقت السلم فالأمر يختلف تماما، حيث تكون شبكات أجهزة الحاسبات موجهة للبناء وليس للقاء، والتعمير وليس التدمير، حيث تسهم أجهزة الحاسب الآلي في زمن السلم في تطوير وتحسين مستوى الأداء في

مختلف نواحي الحياة، كما تسهم في توفير الجهد والطاقة وتقليل تكلفة الإنتاج، كما تعمل بصفة خاصة وهي الأهم علي زيادة الإنتاج في مجالات الزراعة والصناعة وغيرها من المجالات والأنشطة الإنسانية، فضلا عما تقوم به من تحقيق التواصل عن بعد، كعقد المؤتمرات عن بعد، وإبرام الصفقات التجارية عن بعد، والتعليم عن بعد، أو العلاج الطبي عن بعد، وذلك من خلال دمج أجهزة الحاسب بالتليفزيون ووسائل الاتصال، وغير ذلك مما تقوم أجهزة الحاسب أدائه من مهام وافية عالية القيمة في وقت السلم، ففي مثل هذه الحالات إذا قام أحد المخربين من مطوري فيروس الحاسب الآلي بزرع فيروس للحاسب في إحدى شبكات الحاسب فلا يمكن أن يوصف مثل هذا الفعل إلا بأنه جريمة وفقا لأحكام الشريعة التي تقرر مبدأ عدم الإضرار بالغير، وما يرتبط به من تحريم إساءة استعمال المباحات بغرض إلحاق الضرر بالآخرين أو بما لهم من ممتلكات، وهي - أي جريمة فيروس الحاسب - لذلك يجب أن تشملها القوانين العقابية الجديدة في كافة بلدان العالم، خصوصا في ظل الانتشار المتنامي الحالي لشبكات الحاسب في كافة أنحاء المعمورة.

#### جرائم الاحترافات عبر الإنترنت:

وهي من الجرائم التي تقع علي الإنترنت أو التي تكون شبكة الإنترنت هدف المجرم وهي بذاتها المصلحة محل الاعتداء. يعتبر الهجوم علي المواقع واختراقها علي شبكة الإنترنت من الجرائم الشائعة في العالم..

ويشمل هذا القسم جرائم تدمير الواقع، اختراق المواقع الرسمية والشخصية، اختراق الأجهزة الشخصية، اختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه، الاستيلاء علي اشتراكات الآخرين وأرقامهم السرية وإرسال الفيروسات، ولعل جميع الجرائم والانتهاكات معه اختلافها

إلا أنها تجمعها أمرا واحدا وهي كونها جميعا تبدأ بانتهاك خصوصية الشخص، وهذا سببا كافيا لتجريمها، فضلا عن إلحاق الضرر المادي والمعنوي بالمجني عليهم.

هذا ويستخدم المهام في هجومه ما يعرف بالقبلة المنطقية وهي برنامج يدمر البيانات أو قد يستخدم حصان طروادة وهو برنامج لاقتحام أمن النظام يتنكر في شكل برئ حتى يلجإ إلي النظام فيفسده، فيلزم الأمر التطرق إلي شرح لهذه الأفعال وإضرارها<sup>(1)</sup>.

وهذه الأفعال هي:

- الاقتحام أو التسلل:

لكي تتم عملية الاقتحام لابد من برامج يتم تصميمها ليتيح للقائم بهذه العملية والذي يريد اختراق الحاسب الآلي لشخص آخر أن يتم ذلك الاختراق، وقد تم تصميم كثير من هذه البرامج إلا أن معظم تلك البرامج كان بها نقطة ضعف أساسية تقلل كثيرا من إمكانياتها وهي إمكانية الشعور بتلك البرامج علي الجهاز الذي يتم اقتحامه وعليه يكون من الممكن متابعة تلك البرامج والقضاء عليها فيما عدا برنامج استطاع مصمموه التغلب علي هذا العيب وهو برنامج حصان طروادة، ويعتبر هذا البرنامج من البرامج الخطرة علي الإطلاق التي تستخدم في عملية التسلل دون القدرة علي كشفه وتتبعه والقضاء عليه وأهم خصائص أنه يتيح للمخترق أن يحصل علي كلمة السر Password للدخول علي الجهاز بمعنى أنه يتيح بطريقة لا تثير ريبة أو شك. ومن جهة أخرى فإن هذا البرنامج لا يمكن كشفه بواسطة البرامج المتخصصة في كشف الفيروسات. ويقوم هذا البرنامج أيضا بالتجسس علي أعمال المستخدم للجهاز المخترق فهو في أبسط صورة يقوم بتسجيل كل

---

(1) <http://www.Sup4ma.Com/vb/showthread.php?P=7325>

طرقه قام بها علي لوحة المفاتيح منذ أول لحظة للتشغيل ويشمل ذلك كل بياناته السرية أو حساباته المالية أو محادثاته الخاصة علي الإنترنت أو رقم بطاقة الائتمان الخاصة به أو حتى كلمات المرور التي يستخدمها لدخول الإنترنت.

ومن أمثلة هذه الجرائم ما حدث بناء علي بلاغ أمين حزب سياسي بشأن حدوث اختراق لموقع جريدة سياسية وقيام مرتكبي الاختراق ببث عبارات تحمل سباً وقذفاً لبعض النظم الغربية للإيهام بصنورها عنها مما يؤدي للإساءة سياسياً وأخلاقياً للجريدة والحزب المشرف عليها، حيث أن الاختراق حدث علي محتوى صفحة الإنترنت في ٢/٨/٢٠٠٣، وبالفحص تبين أن مرتكبي الاختراق استخدم جهاز حاسب إلي متصل بخط تليفون في القاهرة، وأن وراء ارتكاب الواقعة كلا من "ت. م. ع" ١٧ سنة، "ع. م. ن" ١٦ سنة، وقدمت النيابة العامة المتهمين إلي المحاكمة وتم إعادة الموقع لحالته.

وفي واقعة قام قراصنة أجنبية باقتحام صفحة الإنترنت الإعلامية الخاصة ببنك فلسطين المحدود ووضعوا بها صوراً وشعارات معادية مما اضطر البنك إلي إلغاء الصفحة ومحوها كلياً، وهو أيضاً ما اتضح لوكالة المباحث الفيدرالية FBI أثناء حرب الخليج الأولى عندما أجروا تحقيقاً حول تسلل أشخاص إلي الصفحة العنكبوتية الخاصة بإحدى القواعد العسكرية الأمريكية، وكانت الشكوك قد اتجهت بداية إلي إرهابيين دوليين إلا أن الحقيقة تجلت بعد ذلك في أن المتسللين هما مراققات كانا يعبثان بجهاز الحاسب الآلي في منزلهما.

كما قام متسللين باقتحام النظام الحاسب الآلي الذي يتحكم في تدفق أغلب الكهرباء في مختلف أنحاء ولاية كاليفورنيا الأمريكية حيث استطاعا إلي فصل الكهرباء عن بعض أنحاء الولاية إلي أن تم ضبطهما.



#### - الإغراق بالرسائل:

يلجأ بعض الأشخاص إلى إرسال مئات الرسائل إلى البريد الإلكتروني - E-mail لشخص ما يقصد الإضرار به حيث يؤدي ذلك إلى إغراق المساحة خاصته وعدم إمكانية استقبال أي رسائل، فضلاً عن إمكانية انقطاع الخدمة، حتى يتمكنوا من خلال تلك الأفعال بالإضرار بأجهزة الحاسبات الآلية دونما أي استفادة إلا إثبات تفوقهم في ذلك. فتلك الرسائل قد تكون محملة بملفات كبيرة الحجم لمجرد الإضرار بمستخدم هذا الجهاز نظراً لصغر المساحة المحدودة للبريد الإلكتروني، والتي تصل إلى هذا الجهاز مرة واحدة وفي وقت واحد تقريباً فتؤدي إلى توقعه عن العمل على الفور نظراً لما تسببه من ملء منافذ الاتصال أو من ملء المساحة المتاحة لهذا الجهاز أو المستخدم USER وكذلك من ملء قوائم الانتظار، وبمجرد توقف تلك الأجهزة عن العمل تنقطع بالتالي الخدمة التي تؤديها تلك الأجهزة.

وإذا كان هذا هو الحال الشركات الكبيرة قلنا أن تتصور حال الشخص العادي إذا تعرض بريده لمحاولة الإغراق بالرسائل حيث أنه لن يصمد بريده أمام هذا السيل المتهمر من الرسائل عديمة الفائدة أو التي قد يصاحبها فيروسات أو صور أو ملفات كبيرة الحجم. خاصة إذا علمنا أن مزور الخدمة عادة يعطي مساحة محدودة للبريد الإلكتروني لا تتجاوز عشرة ميجا كحد أعلى.

#### - الفيروسات:

الفيروس هو أحد أنواع برامج الحاسب الآلي إلا أن الأوامر المكتوبة في هذا البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما أو حتى مجرد فتح البرنامج الحامي لفيروس أو الرسالة البريدية المرسل معها الفيروس إصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به.

وقد سمي الفيروس "Virus" بهذا الاسم لتشابه آلية عمله مع تلك الفيروسات التي تصيب الكائنات الحية بعدد من الخصائص كخاصية الانتقال بالعدوي وكونه كائناً غريباً يقوم بتغيير حالة الكائن المصاب وكذا الضرر الذي تسبب فيه في حالة ما إذا تم العلاج بإزالته.

ويمكن تقسيم الفيروسات إلى خمسة أنواع:

الأول: فيروسات الجزء التشغيلي للاسطوانة كفيروس - NEWZLAND.

الثاني: الفيروسات المتطفلة كفيروس VIENNA- CASCADE.

الثالث: الفيروسات المتعددة الأنواع كفيروس TELECOM- FLIP.

الرابع: الفيروسات المصاحبة للبرامج التشغيلية (EXE) أو سواء علي نظام الدوس أو نظام الويندوز.

الخامس: يسمى بحصان طروادة، وهذا النوع يصنفه البعض كنوع مستقل بحد ذاته إلا أنه أدرج هنا كأحد أنواع الفيروسات.

وهنا ينثور التساؤل كيف يتم اقتحام الجهاز؟

لنتم عملية الاقتحام لابد من زرع حصان طروادة، ويتم زرعه بعدة طرق:

١- يرسل عن طريق البريد الإلكتروني كملف ملحق حيث يقوم المستخدم باستقباله وتشغيله وقد لا يرسل وحيداً حيث قد يكون ضمن برامج أو ملفات.

٢- عند استخدام برنامج المحادثة الشهير ICQ وهو برنامج محادثة أنتجته إسرائيل.

٣- عند تحميل برنامج من أحد المواقع الغير موثوق بها.

٤- في حالة اتصال الجهاز بشبكة داخلية أو شبكة الإنترنت.

٥- ينقل بواسطة برنامج TELNET أو FTP.

٦- من خلال بعض البرامج الموجودة علي الحاسب مثل الماكرو الموجودة في برامج معالجة النصوص.

أمريكا تعتمد علي الشركات الخاصة لمواجهة إرهاب "الشبكة"<sup>(١)</sup>:

تقد فشل الأخ الأكبر في المحافظة علي مراقبة تهديد إرهاب الإنترنت عن كثب". هكذا يقول خبراء الأمن. وهم يقولون إن عبء المراقبة والتحسب لهجوم عبر الكمبيوتر علي بنيات تحتية أمريكية حساسة، يقع علي القطاع الخاص، بدلا من الحكومات والجيش.

ويقول دان فيرتون، رئيس التحرير التنفيذي لمجلة "هوم لاند ديفنس ميديا" في الولايات المتحدة، ومؤلف كتاب "التهديد غير المرئي لإرهاب الإنترنت": "إذ سألتني ما إذا كنت راضيا عن الجهود الفيدرالية حول ذلك، فالجواب هو: لا علي الإطلاق" وأضاف: "لدينا حالة غير مسبوقة، فالجزء الأكبر من مصالح أمننا الوطني بين أيدي الشركات الخاصة التي لا تهدف مهمتها إلي حماية الولايات المتحدة، ولكن إلي صنع الأموال وتزويد حملة الأسهم بالقيمة علي استثماراتهم. لم تبد الحكومة أي رغبة في زيادة التشريعات التي يمكن أن تحسن أمن الإنترنت".

ويقول آرثر هلنيك، وهو موظف يعمل في وكالة الاستخبارات الأمريكية منذ ٢٨ عاما، ويدرس الاستخبارات الاستراتيجية في جامعة بوسطن، إن وزارة الأمن الوطني لا تجد التمويل الكافي للتعامل مع إرهاب الإنترنت لأن لديها أولويات أخرى، وإن القطاع الخاص يهتم أكثر بمسألة حماية الشركات.

لكن هذا لا يعني أن الحكومة لا تأخذ التهديد الإرهابي بجدية، وفي الاجتماع السنوي مع الجمعية الأمريكية للأمن الصناعي في أيلول (سبتمبر)

---

(1) <http://www.Aleqt.Com/news.Php?Do=show&id=2069>

الماضي، تم تخصيص ربع الجلسات لمناقشة قضايا الأمن الوطني التي راوحت بين الإرهاب والتجسس المضاد، والتقنيات الناشئة.

ويقول مارك راش، الرئيس السابق لقسم جرائم الكمبيوتر في وزارة العدل الأمريكية: "هناك خطر عام يتعلق بإرهاب الإنترنت، لكن هناك تهديدات مباشرة وفورية أكثر للبنية التحتية، وإذا كانت هناك مبالغ محدودة من الأموال، سأطارد التهديدات الأخرى قبل أن أطارد إرهاب الإنترنت". وقال إن الكثير من الاستراتيجيات التي تتبناها الشركات لحماية أنفسها من المخربين والمتطفلين (الهاكرز) تعمل على خدمتها أيضا إذا قامت منظمات إرهابية، مثل القاعدة، بمهاجمتها.

وقال راش: "نحن نعلم أنهم بذلوا طاقة كبيرة في البحث عن مكامن الضعف والانتكشاف، وجذب الأشخاص ذوي مهارات كشف جرائم الإنترنت والاحتفاظ بهم، بمن فيهم كاتبو الفيروسات، وهذا يدل على أن لديهم الرغبة والمقدرة على إطلاق هجمات على البنية التحتية الإلكترونية" كما تعلم أيضا أن لدينا الغربية في استهداف أنظمة سكادا (أنظمة التحكم الإشرافي والحصول على البيانات) التي تسيطر على أمور العالم الواقعي، مثل فتح أو إغلاق سد، أو ما إذا كان المصعد يتجه إلى الأعلى أو إلى الأسفل".

إلا أن بروس شنيدر، وهو مشفر بارز ومؤسس لشركة كاونتر بان إنترنت سيكيوريتي، يشير إلى أن مثل تلك الهجمات ستحدث فيما بعد. ويتم إهمال التهديد نوعا ما لأنه وكما يشير، مبالغ فيه أيضا. ويقول: "أعتقد شخصيا أن الأمر إلى حد كبير من صنع وسائل الإعلام. نحن نعرف ما هو الإرهاب، إنه طائرات تطير لتصطدم بالبنائات، وليس ذلك ما لا تستطيع الحصول عليه عبر بريدك الإلكتروني، ويضيف: "حتى في أي أمر خطير كالانقطاعات الرئيسية، هناك حجة منطقية بأن انقطاع شبكة الطاقة الأمريكية في الشمال الشرقي عام ٢٠٠٣، كانت نتيجة مشكلة في الكمبيوتر. لكن حتى

لو نفذته القاعدة، فلن يطلتوا عليه إرهاباً، إنه أمر سيء ومكلف، ولكن لن يتم إرهاب أحد".

ويقول هوليك إن البنية التحتية في الولايات المتحدة "آمنة بشكل معقول. وتميل حالات الفشل لأن تكون أخطاء غير معتمدة من قبل أشخاص عليهم أن يعرفوا الأمر أكثر من ذلك". وهو يعرف محاولات من قبل متطوعي إنترنت غير معروفين يدخلون غرف التحكم في مصانع الطاقة نووية مختلفة، ولكن لم تنجح أي منها. وقال: "ربما تستطيع القاعدة أن تشتري شخصين يقومان بذلك مقابل النقود، ولكن وجود جيش من الأوروبيين الشرقيين يموله أسامة بن لادن يحدثون الدمار في العالم أمر لا يمكن التفكير به. اعتقد شخصياً أن هذا بمثابة هلوسة إلى حد كبير".

وأجري هوليك مقابلة مع عالم إسلامي ذي نفوذ مقرب من القاعدة أبلغ أن هناك الكثيرين من الطلبة الإسلاميين الذين يحملون شهادات في علوم الكمبيوتر، ويدعمون تطور الأسلحة عبر الفضاء الإلكتروني من أجل استخدامها ضد الحكومات والاقتصادات الغربية.

ويقول فيرتون إن القاعدة تعلمت من هجمات ٢٠٠١ علي مركز التجارة العالمي، بحيث إنها دمرت عن غير قصد مفتاحي اتصال رئيسيين في قاعدة البناية، وتمكنت من إخراج سوق تبادل الأسهم في نيويورك خارج الشبكة.

وسيعني ذلك احتمال وجود هجمات مستقبلية يتم التنسيق بشأنها لتشمل هجوماً مادياً يعطل البنية التحتية الإلكترونية كما يقول. ويوافق راسنث قائلا: "إن الهجوم عبر الفضاء الإلكتروني المتزامن سيعوق فرص الحكومة للاستجابة. فأنت تفجر بناية في سان فرانسيسكو، وتعطل أنظمة الهاتف أو الإشارات الصوتية في الوقت ذاته".

## الهكرز إرهابيون حسب التصنيف الأمريكي الجديد للإرهاب<sup>(1)</sup>:

حذرت جمعية الحريات المدنية من مشروع قانون أمريكي تقترحه الإدارة الأمريكية يعتبر المتسللين إلى البرامج الكمبيوترية، المعروفين بالهكرز، إرهابيين. وقد أضاف مشروع القانون الجديد مخالفات التسلل إلى برامج الكمبيوتر إلى قائمة الجرائم الإرهابية، وقد تصل عقوبة هذه الجرائم إلى السجن مدة الحياة. ويقول شاري ستيل، مدير مؤسسة إلكترونيك فرونتير، وهي جمعية تدافع عن الحريات المدنية في سان فرانسيسكو، إن اعتبار جرائم الكمبيوتر الصغيرة جرائم إرهابية لا يعتبر ردا مناسباً على الأحداث الأخيرة. وقد تقدم بمشروع القانون الجديد، الذي سيوسع من سلطات متابعة الإرهابيين ومعاقبهم، وزير العدل الأمريكي جون آشكروفت، إثر الهجمات الإرهابية على نيويورك وواشنطن في الحادي عشر من سبتمبر/ أيلول الجاري. وبالإضافة إلى جعل التسلل الكمبيوترية جريمة إرهابية، فإن القانون سيحدد عقوبات تصل إلى السجن مدة الحياة، ويوسع من صلاحيات الاحتجاز والمصادرة قبل الإدانة، بالإضافة إلى إشراك من يساعد المتسللين أو يؤويهم في الجريمة، حتى وإن كانت الأضرار الناتجة عن التسلل ضمن الحد الأدنى. ويقول ستيل إنه يجب أن لا يعاقب المتسلل، الذي لم يحدث ضرراً كبيراً بالسجن بأي حال من الأحوال. ويطبق القانون بأثر رجعي على الجرائم الإرهابية، مما يعني أنه سيؤثر على المتسللين ومصممي برامج الفيروس السابقين، الذين لم يكن القانون ليعاقبهم بأكثر من تحذير أو عقوبة طفيفة، وتشعر جمعيات الحقوق المدنية بالقلق من أن مشروع القانون هذا ربما اقترح باستعجال ودون بحث تأثيراته على الأمن والحريات الشخصية. وتقول لورا ميرفي، من اتحاد جمعيات الحريات المدنية إن علي الكونجرس أن يتخذ

(1) الجزيرة BBC لون لاين.

الإجراءات الكفيلة بحماية البلاد من الهجمات المستقبلية. وأضافت أن الأمريكيين يقيمون الحريات المدنية كثيرا وهي الآن أصبحت في خطر، ودعت الكونجرس إلى التثريب قليلا، وقد حذر المسؤولون والأكاديميون من أن التسلسل التخريبي إلى الإنترنت سيكون جزءا من حرب خطيرة ضد الولايات المتحدة. وقال تقرير حديث لمعهد دراسات الأمن والتكنولوجيا أن معظم التسلسلات السابقة انتهت لها علاقة بالسياسة كانت تسلسلات تهدف الإزعاج وليس الضرر، وإن من غير المرجح أن تنتج مثل هذه التسلسلات عن عمل عسكري أمريكي. ويضيف التقرير أن الاحتمال قائم بأن يحصل تسلسل مدمر ردا على أي عمل تقوم به الولايات المتحدة انتقاما من منغذي الهجوم الإرهابي في الحادي عشر من سبتمبر/ أيلول الجاري، وإن مثل هذا التسلسل الخطير لابد وأن يزعزع شبكات المعلومات في الولايات المتحدة وحلفائها الأوروبيين ويقول مؤيدو قانون مكافحة الإرهاب الجديد إن القانون لا يستهدف المتسللين الشباب.

بعد مرور أكثر من عقدين على دخول فيروسات الكمبيوتر إلى بقعة الضوء وإضافتها إلى أحد أهم الأفعال الإجرامية تأثيرا على الاقتصاد العالمي والتطور العلمي، تتزايد المخاوف من تأثيراتها المدمرة.

"فيروس الحب"، "تشيرنوبيل"، "مايكل أنجلو" و "حصان طروادة" عناوين مشيرة لفيروسات مدمرة باتت مثل قنابل موقوتة تتفجر في الزمن المحدد، وبالضراوة المطلوبة من قبل صانعيها. ويمتد خطرها من الأجهزة الشخصية إلى المؤسسات العسكرية لتذكر مستخدمي الكمبيوتر دائما بعدم الاعتماد بصورة مطلقة على تقدمه التقنية. ويعد برنامج "إلك كلونز" الذي كتبه "رينش سكرينتا" عام ١٩٨٢ أول فيروس تم انتشاره خارج المختبرات، وأصاب الفيروس الأول البرامج العاملة بأنظمة تشغيل "آبل دوس ٣،٣" حيث كان يتم نسخه عن طريق الأقراص المرنة. وظهر "برين" أول فيروس للكمبيوترات

الشخصية عام ١٩٨٦م، والذي تعود حقوقه للأخوة الباكستانيين "باسط وأمجد فاروق علياي" حيث صمماه بفرض حماية برامجها من النسخ غير الشرعي. ونشر مصطلح "فيروس" للمرة الأولى ضمن بحث أكاديمي قدمه "فريد كوهين" عام ١٩٨٤، غير أن رواية الخيال العلمي التي كتبها "ديفيد جبرولد" عام ١٩٧٢م تضمنت وصفا لبرنامج كمبيوتر يسمي "فيروس" يعمل بنفس الآلية التي تعمل بها فيروسات العصر الحالي، ويتم مكافحته ضمن أحداث الرواية بجسم مضاد "أنتي بودي"، كما تحدثت رواية الخيال العلمي لـ "جون برنرز" عام ١٩٧٥ م عن "ديدان وحيدة" تنتشر عبر شبكات الهاتف لتقوم بحذف المعلومات.

ومن هنا فلم يعد مجديا التحدث عن أول ظهور للفيروسات وأول من قام بكتابتها، لأنها بذلك تندرج تحت قائمة الجرائم العلمية التي يتم التخطيط لها وطرحها من خلال الروايات والأفلام السينمائية لقياس ردود الأفعال تجاهها، وإجراء دراسات جدوى لمعرفة الربح الناتج عن توفير حلول لهذه الجرائم، كل ذلك قبل أول ظهور علني لها، يتساوي في ذلك فيروس الكمبيوتر وعمليات استنساخ البشر.

وتمثل الفيروسات أحد أنواع البرمجيات الماكرة، وهي جميع البرامج التي تتسلل إلى نظام الكمبيوتر بدون معرفة ورضا مكرهه، ويكون من الصعب جدا إزالتها بدون خسائر. وتشمل البرمجيات الماكرة إضافة إلى الفيروسات، ديدان الإنترنت وبرامج التجسس.

وتختلف الديدان عن الفيروسات في أنها برامج قائمة بذاتها لا تعتمد على برامج أخرى في أداء عملها، وهي سريعة الانتشار ويصعب التخلص منها نظرا لقدرتها الفائقة على التلون والتناسخ والمراوغة. وتصيب الدودة الجهاز الموصول بشبكة الإنترنت بشكل أوتوماتيكي ومن غير تدخل بشري، الأمر



الذي يجعلها أوسع انتشاراً، ولا تقوم الدودة بحذف أو تغيير الملفات، بل تقوم باستهلاك موارد الجهاز واستخدام الذاكرة بشكل كبير، ينتج عنه بطء شديد في أداء الجهاز. وتكمن خطورة الديدان باستقلاليتها وعدم اعتمادها على برامج أخرى مما يعطيها حرية كاملة في الانتشار السريع، حتى باتت كابوساً مرعباً يلزم كل مستخدم للشبكة.

#### البرامج الماكرة:

ومنذ بداية ظهور الحزمة العريضة للإنترنت بدأ تصميم البرامج الماكرة يركز على دافع ربحي، فمعظم الفيروسات والديدان المنتشرة تم تصميمها للسيطرة على أجهزة المستخدمين بهدف استغلالها لأغراض غير قانونية أو إجرامية، فالأجهزة المصابة بفيروس "زومبي" تم استخدامها لترسل بريداً يحوي مواد ممنوعة كاستغلال القاصرين، أو لابتزاز أصحاب الأجهزة بأشكال عدة.

وعلى الرغم من أن الديدان أصبحت وباء متكرراً لكل مستخدم أجهزة الكمبيوتر، إلا أنها تعد محدودة الضرر نسبياً إذا ما قورنت مع الصيغة الجديدة للبرامج الدخيلة التي ظهرت في السنوات الأخيرة، وهي برامج التجسس التي صممت لتراقب متصفح الإنترنت في جهاز المستخدم وإظهار إعلانات غير مرغوب بها، ونسخ كلمات السر الخاصة به مستغلة ثغرات أمنية في البرمجيات وأنظمة التشغيل.

#### ثغرات أمنية:

وكشفت دراسة لمعهد أمن المعلومات في الولايات المتحدة الأمريكية، أجريت على عينة عشوائية من ٥٠٠ مستخدم ضمن من تعتمد على أجهزة الكمبيوتر في مؤسسات مالية وحكومية وطبية، تسجل ٨٥ في المئة من المشاركين في الدراسة لثغرات أمنية في أنظمتهم خلال فترة ١٢ شهراً على

الأكثر. وقدم ٣٥ في المئة منهم تقارير بالخسائر المالية التي تعرضوا لها جراء هجمات فيروسية وصلت إلى ٣٧٨ مليون دولار، يتضمن ذلك تلف الأجهزة الصلبة وأنظمة التشغيل والبرامج وفقدان معلومات مهمة، وتعطل فترة العمل على الجهاز وتكلفة خبير تقنية المعلومات المشرف على معالجة الحالة. كما أظهرت نفس الدراسة أن وجود برنامج حماية، لا سيما حماية الرسائل الإلكترونية، يمكن أن يوفر ما يصل إلى ٢٥ ألف دولار من الخسائر في كل مرة يصاب فيها جهاز واحد لهذه الشركات.

وبين تقرير لمكتب التحقيق الفيدرالي في الولايات المتحدة أن الخسائر التي تكبدتها الولايات المتحدة المعلوماتية، وصلت إلى ٦٧,٢ مليار دولار.

وحمل التقرير لأصحاب الأعمال التجارية ومستخدمي الكمبيوتر على صعيد العالم أخبارا سارة، فعلى الرغم من أن الهجمات الفيروسية خلال العام ٢٠٠٥م أدت إلى خسائر مالية حول العالم تم تقديرها بـ ١٤,٢ مليار دولار، فإن ذلك يمثل انخفاضاً بنسبة ١٨ في المئة عن خسائر العالم الذي سبقه.

#### التهديد الأكبر:

كما أوضح تقرير للفرقة البريطانية للتجارة والصناعة مؤخراً، أن فيروسات الكمبيوتر تشكل التهديد الأكبر على الأعمال التجارية في بريطانيا. في الوقت الذي أظهر فيه التقرير أن عدد الشركات المصابة بالفيروسات قد تراجع بمقدار الثلث تقريباً منذ آخر دراسة أجريت في عام ٢٠٠٤م. ويمكن السر وراء ذلك في استخدام الشركات لبرامج مكافحة الفيروسات ومعالجة الثغرات الأمنية التي تعاني منها بعض الأنظمة.

ورغم دخول تكنولوجيا المعلومات متأخرة إلى المنطقة العربية، إلا أن مثل هذه الهجمات أدت إلى خسائر بلغت نحو ٦٠٠ مليون دولار خلال العام ٢٠٠٢م، تم التكتّم عليها بشدة من قبل الشركات والبنوك المصابة. ونتيح

برامج مكافحة الفيروسات التي بدأ ظهورها في أوائل الثمانينات، فحص وجود فيروسات في ذاكرة الكمبيوتر أو في قطاع التشغيل. كما تطورت هذه البرامج لاحقاً لتصبح قادرة علي فحص رسائل البريد الإلكتروني للتأكد من سلامتها. وتتضمن آلية عمل برامج مكافحة، مقارنة محتويات الملفات التنفيذية وفحص وجود توقيع لأحد الفيروسات المعروفة ضمن محتويات الملف، ولكنها تبقى ضعيفة في مواجهة أي هجوم فيروسي جديد غير معروف مسبقاً.

#### الشفرة الخبيثة:

وسجل تقرير شركة "سيمانتك" الشرق الأوسط وشمال أفريقيا للعام ٢٠٠٥م تزايد نسبة وقوع الهجمات التي تستهدف الشركات والأجهزة الشخصية بغرض الربح المادي أو السرقة من خلال الكشف عن المعلومات السرية لبطاقات الائتمان أو التفاصيل البنكية، حيث شكلت الشفرة الخبيثة التي ساهمت في الكشف عن المعلومات السرية ٤٧ في المئة من ٥٠ شفرة خبيثة تم إبلاغ "سيمانتك" بها خلال النصف الأول من عام ٢٠٠٥م في منطقة الشرق الأوسط. ويمثل التحول النوعي في أداء البرامج الماكرة، التي صممت في البداية بهدف نشر الفوضى إلي أيقونات دخيلة تهدف إلي التجسس والسرقة، خطراً حقيقياً يصبح معه الاستثمار في برامج مكافحة أوفر بكثير، برغم الميزانيات الضخمة التي يتم رصدها لذلك.

وقدر حجم السوق العالمي لمكافحة الفيروسات خلال العام الماضي ٢٠٠٥م، بحوالي ٢١ مليار دولار، أما سوق الشرق الأوسط فتفوق حصته ١,٤ مليار دولار، وتصنف منطقة الشرق الأوسط علي أنها من المناطق المتقدمة في قطاع تبني حلول مكافحة البرامج الماكرة.

وبلغ إنفاق المملكة العربية السعودية علي تكنولوجيا المعلومات في العام السابق أكثر من ١٩٤ مليار دولار، ويتوقع أن يرتفع هذا الرقم إلي ٢٣٦ مليار دولار بحلول العام ٢٠٠٧م، أي بمعدل نمو سنوي تراكمي نسبته ١٠١ في المئة يخصص جزء رئيسي منه لحماية أمن المعلومات.

وفي الوقت الذي تتجه فيه أصابع الاتهام إلي الشركات الموفرة لحلول مكافحة الفيروسات علي أنها اليد الخفية وراء تنوع وانتشار مظاهر الوباء، تواصل هذه الشركات جني أرباح طائلة تجعلها في مقدمة شركات تكنولوجيا المعلومات قياسا بالعائدات السنوية.

وتحتل شركة "سيمانتك" مكانة متقدمة، ضمن شركات تكنولوجيا المعلومات الأكثر ربحا، حيث بلغت عائداتها في السنة المالية المنتهية في شهر إبريل ٢٠٠٤م ما قدر بـ ١,٨٧ مليار دولار، ويتوقع أن تبلغ عائداتها في نهاية السنة المالية الحالية والتي تمتد إلي إبريل ٢٠٠٦م، ما يصل إلي ٤,٠٧ مليار دولار، وفي سياق خلق تكتلات في قطاع مكافحة الفيروسات ودمج أحدث التقنيات، أنهت الشركة في شهر سبتمبر الماضي صفقة شراء لشركة "هيرتس" المنتجة لبرامج الفيروسات أيضا، بلغت قيمتها ١١ مليار دولار، وعليه تتوقع "سيمانتك" أن ترتفع عائداتها خلال العام ٢٠٠٧م إلي ٥,٣٥ مليار دولار، وتشتهر "سيمانتك" ببرامجها "تورتن أنتي فيروس" و "تورتن كوماندور" و "تورتن إنترنت سيكيورتي" و "تورتن أنتي سبام" و "تورتن فايرول".

وتعد شركة "مكافي" من الشركات البارزة في قطاع تطوير برامج مكافحة الفيروسات، وحققت الشركة في الربع الرابع من العام الماضي فقط، ربحا صافيا وصل إلي ٣٩,٧ مليون دولار، حيث بلغت العائدات الكلية للشركة خلال العام ٢٠٠٥م ما قيمته ٩٨٧,٣ مليون دولار، وذلك بارتفاع بنسبة ٨ في المئة عن العام ٢٠٠٤م.

وبالنظر إلى حجم الإنفاق المتوقع في قطاع مكافحة البرامج الماكرة خلال السنوات المقبلة، والذي ينشئ بتنامي هذا القطاع في العديد من الدول العربية، في مقدمتها مصر والمملكة العربية السعودية والإمارات بنسب تتراوح ما بين ٢٠ و ٣٠ في المئة، تظهر الحاجة إلى توفير أنظمة أمن معلومات عربية، خاصة بالنسبة للمؤسسات الاستراتيجية الحساسة، وإلى أهمية الاستثمار في هذا المجال: مكافحة البرمجيات الماكرة وأمن المعلومات.

ليلة القبض على فايرس مليسا<sup>(١)</sup>:

قد تم اعتقال ديفيد سميث ٣٠ عاما من قبل FBI ويعمل كمبرمج كمبيوتر في مختبرات At & T في فلورهام بارك وأيضا مستشار موقع On- Site Consultant بعد أن استطاعت المباحث الفيدرالية من تتبع أثره بالتعاون مع فنيين من شركة أمريكا أون لاين.

وكانت أمريكا أون لاين هي التي اتصلت بالمباحث لإخبارهم بعد أن أدي بحث الشركة الداخلي الخاص إلى الإشارة إلى أن مصدر الفايرس مليسا من نيوجيرسي كان ذكر كرستوفر بوب رئيس وحدة تحليل الكمبيوتر.

وقد ذكر جريدة نيويورك تايمز أن السلطات الأمنية قد تتبعت مصدر أول نسخة من فايرس مليسا إلى حساب إنترنت مع شركة مونماوث إنترنت كورب في ريد بانك في نيوجيرسي، وبعد ذلك تتبعت الأثر إلى تلفون سميث وكانت شركة مونماوث قد أعطت للسلطات كشفا كاملا بأسماء الذين استخدموا الإنترنت يوم ٢٦ مارس، اليوم ظهرت فيه المليسا كما أكد ذلك مارك ستيفن مدير العمليات في الشركة ويبدو أن سميث تملكه الرعب بعد إصدار FBI لتحذيرات من الفايرس قام برمي كمبيوتره الشخصي في

(1) <http://www.2alsaha.Com/sahat/Forum7/HTML/003737.html>.

صندوق القمامة في المجمع السكني الذي يسكن فيه محاولاً بذلك التخلص من أي أثر يقود إليه.

وكان خبراء الكمبيوتر قد استخدموا الرقم التعريفي الفريد Unique Identification Number يكون مدمجاً في المستندات لتتبع فايرس مليسا إلي أمتب فايروسات مشهور يطلق علي نفسه أسم فيكودين- أي- أس VicodenES، ولكن السلطات أكدت أن سميث ليس الشخص المعروف بتلك الأرقام المميزة، وتعتقد السلطات أن سميث قد استخدم فايرس كتبه فيكودين- أي- إس ودمجه بفايرس آخر لينشأ فايرس المليسا، وفيكون اسم لدواء قاتل للأكم. أما ستيفن الثمان محامي المعتقل ديفيد سميث (اعتقل الخميس الماضي) فقد ذكر يوم السبت الماضي أن سميث لم يكن ينوي أن يتسبب في أي خراب لأي كمبيوتر، وأنه خطأ علي أنه كمبيوتر هاكلز خطير وبالتالي وقع ضحية الحملة الحكومية علي جرائم التكنولوجيا المتطورة Hi tech Crimes و أضاف المحامي الثمان "أن عالم الكمبيوتر عالم إجراء التجارب كل يوم تقريباً، ولم يقم بعمل أي شيء أو نوى عمل شيء بنية سيئة، وأضاف المحامي الثمان "أنه حزين جداً"، وخائف ومضطرب، لقد كانت هذه تجربة مرعبة، لقد ذهبوا إليه كعصابة اختطاف، السلطات المحلية والشرطة و FBI ، لقد تعاملوا معه كأنه تيد باندي ويقتصد بذلك القاتل الذي أعدم قبل ١٠ سنين في فلوريدا.

ويواجه ديفيد سميث تهم تعطيل الاتصالات العاملة والتآمر وسرقة خدمات الكمبيوتر، تهم تحمل عقوبات تصل إلي سجن ٤٠ سنة وغرامة ٤٨٠ ألف دولار أي ما يقارب نصف مليون دولار، وكان إطلاق سراح ديفيد سميث بكفالة مقدارها ١٠٠ ألف دولار يوم الجمعة الماضي<sup>(١)</sup>.

(١) عن جريدة الرأي العالم الكويتية ١٤-٤.

#### حالات عملية شهيرة من واقع الملفات الفضائية:

قضية مورس: هذه الحادثة هي أحد أول الهجمات الكبيرة والخطرة في بيئة الشبكات ففي تشرين الثاني عام ١٩٨٨ تمكن طالب يبلغ من العمر ٢٣ عاما ويدعى ROBER MORRIS من إطلاق فايروس عرف باسم (دودة مورس) عبر الإنترنت، أدى إلي إصابة ٦ آلاف جهاز يرتبط معها حوالي ٦٠٠٠٠ نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات والنواير الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار إضافة إلي مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم علي مورس بالسجن لمدة ٣ أعوام وعشرة آلاف دولار غرامة.

قضية الجحيم العالمي: تعامل مكتب التحقيقات الفدرالية مع قضية أطلق عليها اسم مجموعة الجحيم العالمي GOLOBAL HELL فقد تمكنت هذه المجموعة من اختراق مواقع البيت الأبيض والشركة الفدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية، وقد أدین اثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة، وقد ظهر من التحقيقات أن هذه المجموعات تهدف إلي مجرد الاختراق أكثر من التدمير أو النقاط المعلومات الحساسة، وقد أمضي المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشركة وتتبع آثار أنشطتها، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة.





## **الفصل الثاني**

### **الجرائم المعلوماتية**



## الجرائم المعلوماتية

### وجرائم الكمبيوتر

### Computer Crimes

### والإنترنت

### Cyber Crime

لا شك أن اصطلاح جرائم الكمبيوتر والإنترنت هو مصطلح يشمل كافة الجرائم المستحدثة والمتعلقة بكل من الكمبيوتر أو شبكة الإنترنت.

فهذا المصطلح من العمومية بحيث يشمل كافة الجرائم المتعلقة بالحاسبات سواء كانت الحاسبات هي التي يقع عليها فعل الاعتداء أو الجرائم التي تكون فيها الحاسبات أداة في يد الفاعل مرتكب جريمة الاعتداء وهذا الاصطلاح من العمومية بحيث يشمل كافة الأفعال والاستخدامات العديدة التي يصعب حصرها لشبكة الإنترنت العملاقة من الناحية التقنية.

وهذا المصطلح يشمل أيضا مضمون ما ثبته أو يكون موجود علي تلك الشبكة من بيانات أو معلومات أي الجرائم التي تقع علي ذلك المضمون المعلوماتي.

ولكن هناك تداخل بين كافة المصطلحات وارتباط لا يمكن إنكاره إذ يستحيل فصل تلك المصطلحات عن بعضها البعض.

علاوة علي ما تقدم فإن هناك ترابط بين كل من الحوسبة والاتصال إذ لا يمكن فصل كل من تقنية الحوسبة عن تقنية الاتصال في عصر المعلومات فائقة السرعة إذ أن الحوسبة تقوم علي استخدام وسائل التقنية لإدارة وتنظيم معالجة البيانات أما الاتصال فهو قائم علي وسائل نقل تلك المعلومات بكافة دلالتها الدارجة والمعرفة.

ومن الجدير بالذكر أن نشير إلى أن اصطلاح الحوسبة والاتصال المتلازمين أدى إلى أن إطلاق البعض عليهم تقنية المعلومات INFORMATION TECHNOLOGY التي تعرفها منظمة اليونسكو بأنها تلك الفروع العلمية والتقنية والهندسية المستخدمة في تداول ومعالجة المعلومات والبيانات وفي تطبيقها والمرتبطة بالحاسبات في إطار استخدام الإنسان لها لتحقيق حاجاته الاجتماعية والثقافية والاقتصادية.

ومن الجدير بالذكر أن الاعتداء الواقع على تلك البيانات والمعلومات بالشكل السالف بيانه يطلق عليه الجرائم المعلوماتية وهي الترجمة الحرفية لمصطلح INFORMATIQUE أو الاعتداء الواقع على المعالجة الآلية للبيانات.

ولا يفوتنا أن نشير إلى أن هناك نوعا منبثق عن تلك الجرائم المعلوماتية والإجرام الاقتصادي Computer- Related Economic Grime وهي الجرائم التي تستهدف تلك المعلومة الاقتصادية.

وكذلك هناك نوع آخر من الإجرام المعلوماتي يطلق عليه البعض مصطلح سينمائي وإعلامي وهي اصطلاح جرائم ذوي الياقات البيضاء white Collar Crime. وهو اصطلاح فقهي قديم كان يطلق على الجرائم التي يرتكبها المثقفون وأهل العلم بصفة عامة وقد اقتبسها الكثيرون لا سيما بعد ثورة المعلوماتية الحالية وتلك الجرائم يكون هدفها دائما مثل كافة الجرائم المرتبطة بالحاسبات الكمبيوتر وما يحمله من بيانات ومعلومات ويشير البعض إلى أن من الأفضل إطلاق اسم جرائم Cyber Crime على كافة جرائم الكمبيوتر وجرائم الشبكات وذلك لأن كلمة Cyber جامعة لكافة الجرائم التي تتم عبر شبكة الإنترنت العملاقة.

ولكننا نشير إلى أنه من الأفضل استخدام مصطلح جرائم الكمبيوتر والإنترنت Computer crime- Cyber Crime لأنه يشمل كافة الجرائم التي تقع على الحاسبات بصفة عامة أو التي تستخدم فيها الحاسبات كأداة للجريمة التي يكون مضمونها في الغالب الاعتداء على المعلوماتية الموجودة على شبكة الإنترنت بما تحتوي من معلومات وبيانات.

وعلى أي الأحوال هناك صعوبة في الفصل بين كل من جرائم الحاسبات وجرائم الإنترنت ذلك لأن تلك الجرائم تستهدف مركز معالجة البيانات المخزنة في الحاسب الآلي وتستغلها بطريقة غير مشروعة مثل استغلال أرقام ورموز بطاقة الائتمان.

وكذلك يمكن أن تقع الجريمة على البيانات المخزنة في الحاسب الآلي بقصد التلاعب بها وتدميرها بواسطة الفيروسات المرسلة عبر البريد الإلكتروني لذلك ينصح دائما بوضع برنامج حماية من الفيروسات حتى يضمن عدم تعرض الحاسب إلى مثل تلك الفيروسات المدمرة للبيانات وإتلافها.

وخلاصة القول أنه يصعب في ظل التقنية العالية وعصر المعلومات فائقة السرعة حصر المخاطر الأمنية بصفة عامة ذلك لأن كل يوم هناك مخاطر جديدة مبتكرة ولا تقف عند زمن معين أو محدد.

ولا شك أن هناك جرائم يستخدم فيها الإنترنت لهدم القيم الاجتماعية لدى بعض المجتمعات لا سيما في الدول النامية والمتخلفة سواء كانت تلك القيم الاجتماعية راقية أو بالية الأمر الذي يؤدي إلى تقدم تلك المجتمعات في حال اختيار أفرادها للبرامج والبيانات التي تدفع إلى التقدم والرقى أو تكون تلك المجتمعات عرضة للتفشي والانحلال في حالة إقبال أفرادها المحرومين من

بعض الحريات علي المواقع الهدامة التي تحرض الأفراد علي التمرد علي الواقع الذي تعيشه وكانت تعتبره إلي زمن طويل قدر لا محالة في تغييره. أما مجرمو الإنترنت والكمبيوتر أما أن يكونوا عاملون علي أجهزة الحاسب الآلي في منازلهم أو موظفون ساخطون علي الشركات التي يعملون فيها ولديهم الرغبة في تدمير الجهاز وإتلافه أو سرقة ماديها أو معلوماتياً. أو أن يكون مجرم النت والكمبيوتر من العابثين أو ما يعرفون بمسمي المتسللين الهواة العابثين بقصد التسلية أو المحترفين المخترقين لتلك الأجهزة وما عليها من بيانات.

وهناك نوع من المجرمين يكونوا في شكل تشكيل عصابي يهدف إلي ارتكاب جريمة منظمة لسرقة البيانات أو تعطيل شبكة الإنترنت العملاقة وذلك بخلقهم أنواعا من الفيروسات علي ما سنري.

ولا يفوتنا أن نشير إلي أن هناك جرائم ومجرمون يستخدمون أحدث ما وصل إليه العمل في تنفيذ جرائمهم وذلك بالاستعانة بالتقنية العالمية التي وصل إليها الإنسان في أجهزة أخرى ذات صلة بتلك الجرائم وهي ما يطلق عليها الجرائم ذات التقنية العالية التي يستخدم فيها الهاتف المحمول (البلوتوث) في التصوير والتسجيل أو استخدام أجهزة تصنت.

فجرائم المعلوماتية المقصود بها جميع أوجه الاعتداء الإلكتروني الموجهة للمعلوماتية مثل سرقة البيانات المعلوماتية وجرائم الملكية الفكرية ونحوها من الأساليب الإجرامية الإلكترونية الموجهة لقواعد البيانات والمعلومات.

أما جرائم الكمبيوتر فهو مصطلح شامل أشمل من المصطلح السابق ويقصد فيه كل الجرائم التي يستخدم فيها الكمبيوتر سواء أداة الجريمة أو كان هدف الجريمة ويدخل من ضمنها جرائم المعلوماتية وجرائم الإنترنت، كما

يدخل من ضمنها الاعتداء على الشبكات المحلية الخاصة بالهيئات والمنشآت الخاصة والعامة.

أما جرائم الإنترنت فهو مصطلح يقصد به كل جريمة أو أسلوب إجرامي إلكتروني تستخدم فيه الإنترنت كوسيلة لتنفيذه ويدخل من ضمن ذلك الجرائم المادية التي ارتبطت بأسباب ووسائل إلكترونية تمت عبر الإنترنت مثل ترويج المخدرات وبيع السلع المسروقة عبر الإنترنت ونحو ذلك.

هناك مصطلح رابع يقال له جرائم التقنية العالية وهذا أشمل من الجميع يدخل من ضمنه كل الأنواع السابقة ويزيد على ذلك بعض الجرائم الإلكترونية الأخرى التي تتم بغير الكمبيوتر أو الإنترنت مثل جرائم الجوال واستخدام التكنولوجيا في تنفيذ الأسلوب الإجرامي الإلكتروني مثل استخدام أجهزة سرية للتصنّت أو لنشر أوبئة بيولوجية ونحوها أو التصنّت عبر الأقمار الاصطناعية.

#### الجرائم الإلكترونية:

الجريمة الإلكترونية: هو ببساطة استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين.

ومن الأمثلة على الإرهاب الإلكتروني هو نفاذ الهاكر إلي سجلات مريض في أحد المستشفيات، والتلاعب بهذه السجلات بحيث يؤدي ذلك إلي حقن المريض مثلاً بجرعة زائدة من دواء لا يتقبله جسمه.

تعريف: كل أسلوب غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات\*.

ولا شك في أن اتجاه وكالات المباحث والاستخبارات في شتى الدول بعد حدوث أي حادث فإنها ترغب في الحصول علي حريات أكبر في تعقب المعلومات الرقمية.

وهذا دليل على أهمية الشبكات الرقمية في عالم اليوم، وخطورتها إذا ما استخدمت بالشكل غير الصحيح.

#### دور الكمبيوتر في الجريمة:

يلعب الكمبيوتر ثلاثة أدوار في ميدان ارتكاب الجرائم، ودورا رئيسا في حقل اكتشافها.

#### ففي حقل ارتكاب الجرائم يكون للكمبيوتر الأدوار التالية:

- قد يكون الكمبيوتر هدفا للجريمة.
- قد يكون الكمبيوتر أداة الجريمة لارتكاب جرائم تقليدية.
- قد يكون الكمبيوتر بيئة الجريمة.

#### أما من حيث دور الكمبيوتر في اكتشاف الجريمة:

التحقق الاستدلالي لكافة الجرائم، عوضا عن أن جهات تنفيذ القانون تعتمد على النظم التقنية في إدارة المهام من خلال بناء قواعد البيانات ضمن جهاز إدارة العدالة والتطبيق القانوني.

#### الحماية من الجرائم الإلكترونية:

قام الرئيس الأمريكي بيل كلينتون في العام ١٩٩٦ بتشكيل لجنة حماية منشآت البنية التحتية الحساسة [www.nipc.gov](http://www.nipc.gov)

وكان أول استنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والاتصالات إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة.

وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف الأول لأية هجمات تستهدف أمن الولايات المتحدة.



## الحرب الرقمية من المنظور الأمريكي:

تقتبس فيما يلي التعريف الذي تعتمد عليه كليات الحرب الأمريكية، وتدعوه بهجمات الشبكات الكمبيوترية، وتصنفه تحت بند "العمليات الإلكترونية". ويقول التعريف بأن الحرب الرقمية هي:

"الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها".

وحسب التعريف فإن العمليات الإلكترونية تتضمن أنشطة مثل أمن العمليات، والعمليات النفسية، والخداع العسكري، الهجمات الفيزيائية، والهجمات على شبكات الكمبيوتر.

وهناك الكثير من الطرق التي يمكن من خلالها تنفيذ الهجمات الرقمية:

- الهجمات المباشرة من خلال التدمير الفيزيائي لأجهزة الخصم.
- باستخدام القوة العسكرية المباشرة.
- سرقة المعلومات من أجهزة الخصم.
- استخدام الفيروسات.

## سيناريوهات حروب المعلومات:

وكما هي الحال في أية حرب، فإن الجيوش المتصارعة تستهدف دوما ثلاثة عناصر أساسية من أجل كسب المعركة، وهي العناصر العسكرية، والاقتصادية، والسياسية أو بكلمات أخرى إرادة الشعب.

وفي عالم حروب المعلومات تجد العناصر الثلاث نفسها وعلي رأسها مراكز القيادة والتحكم العسكرية، والبنوك والمؤسسات المالية. ومؤسسات المنافع كمؤسسات المياه والكهرباء وذلك لإخضاع إرادة الشعوب.

### الهجمات على الأهداف العسكرية:

تستهدف هذه النوعية من الهجمات عادة، الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات.

وهذا النوع من الهجمات نادر الحدوث عادة لعدة أسباب:

- أولها هو أنه يتطلب معرفة عميقة بطبيعة الهدف.
- وطبيعة المعلومات التي يجب النفاذ إليها، وهي معرفة لا تمتلكها إلا الحكومات.

- إضافة إلى أن الحكومات تقوم عادة بعزل المعلومات العسكرية الحساسة عن العالم، ولا تقوم بوصل الأجهزة التي تحملها بالعالم الخارجي بأي شكل من الأشكال.

ولكي يبقى الحذر واجبا من عمليات التخريب الداخلية، ومن هنا تأتي ضرورة وضع نظم موثوقة للتحقق من شخصيات المستخدمين، والتحديد الدقيق لطبيعة المعلومات التي يسمح بالنفاذ إليها.

ومن السيناريوهات التي تمثل هذا النوع من الهجمات، هو النفاذ إلى النظم العسكرية واستخدامها لتوجيه جنود العدو إلى نقطة غير آمنة قبل قصفها بالصواريخ مثلا.

### الهجمات على الأهداف الاقتصادية:

أصبح الاعتماد على شبكات الكمبيوتر شبه مطلق في عالم المال والأعمال، مما يجعل هذه الشبكات، نظرا لطبيعتها المترابطة، وانفتاحها على العالم، هدفا مغريا للعابثين والهكرة.

ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل كبير بالانطباعات السائدة والتوقعات، والتشكيك في صحة هذه المعلومات، أو

تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة، وإضعاف الثقة في النظام الاقتصادي. ولذلك فإن الهجمات ضد نظم المعلومات الاقتصادية يمكن لها أن تكون مؤذية جدا.

ومن الأمثلة على الهجمات الاقتصادية هي العملية التي قامت بها مجموعة من الهكرة، تعرف باسم نادي الفوضى، في عام ١٩٩٧: حيث قام هؤلاء بإنشاء برنامج تحكم بلغة آكتف إكس مصمم للعمل عبر إنترنت ويمكنه خداع برنامج كويكن Quicken المحاسبي بحيث يقوم بتحويل الأموال من الحساب المصرفي للمستخدمين. وباستخدام هذا البرنامج أصبح بإمكان هؤلاء الهكرة سرقة الأموال من أرصدة مستخدمي برنامج كويكن في جميع أنحاء العالم. وهذه الحالة هي مثال واحد فقط على الطرق التي يمكن بها مهاجمة شبكات المعلومات الاقتصادية واستغلالها، وهي طرق يمكن أن يكون لها آثار مدمرة على المجتمعات.

#### سبل الحماية:

- يمكننا أن ندخل هنا في مواضيع شتى حول سبل حماية نظم المعلومات الهامة، ولكن تبقى الخلاصة هي أنه لا يمكن تقديم حماية مطلقة وتامة لنظم المعلومات المرتبطة بشبكات الاتصالات.
- والسبيل الوحيد لتأمين المعلومات الحساسة هو عزل الأجهزة التي تحتوي هذه المعلومات عن العالم.
- ولكن مثل هذه الإجراءات يمكن لها تؤدي إلى نتائج أكثر إيذاء على المدى الطويل تتمثل في حرمان المجتمع من وسائل زيادة الإنتاجية والفعالية.

- ومع ذلك، فإن استخدام مجموعة من الإجراءات الأمنية الأساسية يمكن لها أن تقلل بشكل كبير من مخاطر الاختراقات والإرهاب الإلكتروني.
- وتشمل الإجراءات الأمنية التي يجب مراعاتها ثلاث نواح هامة يجب تغطيتها جميعا وبشكل متكافئ، وإلا فإن السياسة الأمنية ستعتبر فاشلة.
- تأمين خطوط الدفاع الأمامية باستخدام تطبيقات الجدران النارية (بتأمين المنافذ Ports).
- تأمين حسابات المستخدمين ونظم التحقق من الهوية (كلمات السر وأسماء المستخدمين، .....).
- خدمات الأدلة (قواعد بيانات خاصة، أسماء مستخدمين كلمات مرور، سمات بيولوجية).
- تقنية المفاتيح العام.
- الشبكات الافتراضية الخاصة (قناة خاصة وسيطة عبر الشبكة العامة).
- أمن البرمجيات.

#### الأساليب التقنية:

- تنزيل برامج ترقية من الموقع المعتمدة علي الإنترنت.
- حذف كل الملفات التي تنزل في الجهاز أثناء ارتباطه بالإنترنت، وملفات الإنترنت المؤقتة والمحفوظات بشكل دوري.
- منع أي تحركات مشبوهة عند الدخول إلي أي موقع غير موثوق.
- اعتماد تنوع مصادر الأجهزة والبرامج من أجل كسر عامل الاحتكار.
- استخدام برامج الحماية بشكل ملزم.
- استخدام برامج تتبع مصدر الرسائل الإلكترونية.

- الاستفادة من تقنيات التعرف علي شخصية مرتكب جريمة نظم المعلومات وعنوان IP.

- التعرف علي نقاط ضعف الشبكة ومعالجتها.

- استخدام بصمة الإصبع بديلا أمثل لكلمة المرور.

#### محاربة جرائم الإنترنت:

جلبت التجارة علي الإنترنت الجرائم إلي الإنترنت. وقد طورت وكالات تطبيق القوانين أساليب جديدة وعلاقات جديدة للقبض علي المجرمين في الفضاء السيبراني، أو الإنترنت<sup>(1)</sup>.

مركز الشكاوي الخاصة بجرائم الإنترنت (IC3) هو كناية عن نظام تبليغ وإحالة لشكاوي الناس في الولايات المتحدة والعالم أجمع ضد جرائم الإنترنت. ويخدم المركز، بواسطة استمارة للشكاوي مرسلة علي الإنترنت وبواسطة فريق من الموظفين والمحليلين، الجمهور ووكالات فرض تطبيق القوانين الأمريكية والدولية التي تحقق في جرائم الإنترنت.

والمقصود بجرائم الإنترنت، المسماة أيضا الجرائم السيبرانية أو السبرانية، هو أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الإنترنت، مثل مواقع الإنترنت، وغرف المحادثة، أو البريد الإلكتروني. ويمكن أن تشمل جرائم الإنترنت أيضا أي أمر غير مشروع، بدءا من عدم تسليم البضائع أو الخدمات، مروراً باقتحام الكمبيوتر (التسلل إلي ملفات الكمبيوتر)، وصولاً إلي انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي (سرقة الأسرار التجارية)، والابتزاز علي الإنترنت، وتبييض الأموال

(1) دانيال لاركين رئيس وحدة في مركز الشكاوي الخاصة بجرائم الإنترنت (IC3) في مكتب التحقيقات الفيدرالي.

الدولي، وسرقة الهوية، وقائمة متنامية من الجرائم الأخرى التي يسببها الإنترنت.

#### الجريمة تدخل إلى الإنترنت<sup>(١)</sup>:

نشأ مركز الشكاوي الخاصة بجرائم الإنترنت كمفهوم سنة ١٩٩٨ بإدراك ملائم بأن الجريمة بدأت تدخل الإنترنت لأن الأعمال التجارية والمالية كانت قد بدأت تتم عبر الإنترنت، ولأن مكتب التحقيقات الفيدرالي أراد أن يكون قادراً على تعقب هذه النشاطات وعلي تطوير تقنيات تحقيق خاصة بجرائم الإنترنت.

ولم يكن هناك آنذاك أي مكان واحد يمكن للناس التبليغ فيه عن جرائم الإنترنت، وأراد مكتب التحقيقات الفيدرالي التمييز بين جرائم الإنترنت والنشاطات الإجرامية الأخرى التي تبلغ عنها عادة الشرطة المحلية ومكتب التحقيقات الفيدرالي والوكالات الأخرى التي تطبق القوانين الفيدرالية وهيئة التجارة الفيدرالية (FTC) والمكتب الأمريكي للتفتيش البريدي (USPIS)، وهو الشعبة التي تطبق القوانين المتعلقة بمصلحة البريد الأمريكية، وغيرها من الوكالات.

وقد تم تأسيس أول مكتب للمركز سنة ١٩٩٩ في مورغانتون بولاية وست فرجينيا، وسمي مركز شكاوي الاحتيال علي الإنترنت. وكان المكتب عبارة عن شراكة بين مكتب التحقيقات الفيدرالي والمركز القومي لجرائم موظفي المكاتب، وهذا الأخير مؤسسة لا تبغي الربح متعاقدة مع وزارة العدل الأمريكية مهمتها الأساسية تحسين قدرات موظفي أجهزة تطبيق القانون، علي صعيد الولاية والصعيد المحلي، علي اكتشاف جرائم الإنترنت أو الجرائم الاقتصادية ومعالجة أمرها.

(١) <http://usinfo.State.Gov/journals/itgic/0306/ijga/larkin.Htm>.

وفي العام ٢٠٠٢، وبغية توضيح نطاق جرائم الإنترنت التي يجري تحليلها، بدءاً من الاحتيال البسيط إلى تشكيلة من النشاطات الإجرامية التي أخذت تظهر على الإنترنت، أعيدت تسمية المركز وأطلق عليه اسم مركز الشكاوي الخاصة بجرائم الإنترنت، ودعا مكتب التحقيقات الفيدرالي والشرطة السرية وغيرها، للمساعدة في تزويد المركز بالموظفين وللمساهمة في العمل ضد جرائم الإنترنت.

وقد أصبح هناك اليوم في مركز الشكاوي القائم بغيرمونت، بولاية وست فرجينيا، ستة موظفين فيدراليين وحوالي أربعين محلاً من القطاع الأكاديمي وقطاع صناعة الكمبيوتر وخدمات الإنترنت يتلقون الشكاوي المتعلقة بجرائم الإنترنت من الجمهور، ثم يقومون بالبحث في الشكاوي وتوضيب ملفها وإحالتها إلى وكالات تطبيق القانون الفيدرالية والمحلية والتابعة للولايات وإلى أجهزة تطبيق القانون الدولية أو الوكالات التنظيمية وفرق العمل التي تشارك فيها عدة وكالات، للقيام بالتحقيق فيها.

وبإمكان الناس من كافة أنحاء العالم تقديم شكاوي بواسطة موقع مركز الشكاوي الخاصة بجرائم على الإنترنت ([http:// www. Ic3. gov](http://www.Ic3.gov)). ويطلب الموقع اسم الشخص وعنوانه البريدي ورقم هاتفه؛ إضافة إلى اسم وعنوان ورقم هاتف والعنوان الإلكتروني، إذا كانت متوفرة للشخص، أو المنظمة، المشتبه بقيامه بنشاط إجرامي، علاوة على تفاصيل تتعلق بكيفية وقوع الجريمة حسب اعتقاد مقدم الشكاوي ووقت وقوعها وسبب اعتقاده بوقوعها، بالإضافة إلى أي معلومات أخرى تدعو الشكاوي.

#### إعداد ملفات القضايا لإحالتها:

هدف عمليات المركز الرئيسي هو أخذ شكاوي المواطن الفرد التي قد تتعلق بجريمة تنجم عنها أضرار حدود ١٠٠ دولار مثلاً، وضمها إلى

المعلومات المبلغ عنها من جانب ١٠٠ أو ١٠٠٠ ضحية أخرى من مختلف أنحاء العالم، فقدت أموالا نتيجة نفس السيناريو، وثم إعداد ملف قضية مهمة بأسرع وقت ممكن.

والحقيقة هي أنه لا يسمح لمعظم وكالات فرض تطبيق القانون معالجة أمر القضايا التي تمثل مبالغ ضئيلة نسبيا، ومبلغ مئة دولار أقل علي الأرجح من المبلغ المسموح بالتحقيق في أمره. غير أن معظم المجرمين يعملون علي الإنترنت لكي يوسعوا نطاق فرصهم في إيذاء الضحايا وكسب المال، وجرائم الإنترنت لا تقتصر أبدا تقريبا علي ضحية واحدة. وهكذا، إذا تمكن محققو مكتب الشكاوي من ربط عدة شكاوي ببعضها البعض، وحولوها إلي قضية واحدة قيمتها عشرة آلاف أو مئة ألف دولار، أضرت بمئة أو ألف ضحية تصبح الجريمة عندئذ قضية أكثر أهمية، ويصبح بإمكان وكالات تطبيق القانون التحقيق فيها.

ويساعد مركز الشكاوي الخاصة بجرائم الإنترنت أحيانا وكالات تطبيق القانون من خلال إجراء الأبحاث وإعداد ملف القضية الأولى. وقد وجد محققو المركز، خلال السنتين والنصف الأولتين من عمر المشروع، وعلي الرغم من جهود إعداد القضايا وإحالتها بسرعة إلي وكالات تطبيق القوانين، أن فرق العمل الخاصة بمكافحة جرائم الإنترنت لم تكن جميعا مجهزة لمتابعة هذه الجرائم أو التحقيق فيها بسرعة، وقد لا تملك بعض فرق العمل هذه القدرة علي القيام بعمليات سرية، أو قد لا تملك التجهيزات اللازمة لاقتفاء الآثار الرقمية للأدلة الجرمية التي يحولها إليها مركز الشكاوي. لذلك، أصبح من المهم جدا بالنسبة لمركز الشكاوي أن يطور ويتعقب آثار الجرائم التي يتوصل إلي إعداد ملف القضية الأولى، مثلا، قد يتعرف مركز الشكاوي الخاصة بجرائم الإنترنت علي هوية ١٠٠ ضحية، ويقرر أنه يبدو أن النشاط الإجرامي صادر عن جهاز مقدم خدمات كمبيوتر في كندا، مثلا، لكن ذلك



الجهاز قد يكون مجرد كمبيوتر تم التسلل إليه. وقد يكون ما حدث هو أن المجرمين يستخدمون هذه الآلة "كنقطة انطلاق وهمية" لإخفاء مكان تواجدهم الحقيقي. لذا فإنه من المفيد بالنسبة لمحللي مركز الشكاوي أن يعرفوا المزيد عن "نقطة الانطلاق الوهمية"، فقد تكون هناك مجموعة في تكساس، أو أفريقيا الغربية، أو رومانيا، تستخدم جهاز مقدم خدمات الإنترنت في كندا لجمع المعلومات عن الضحايا المحتملين.

#### تحالفات الصناعة:

نظرا لتوصل مركز الشكاوي الخاصة بجرائم الإنترنت IC3 إلى أنه من الأفضل في بعض القضايا التقنية المعقدة تعقب أثر التحقيقات المبكرة، قام بإنشاء مكتب فرعي لهذا الغرض في بيتسبرغ، بولاية بنسلفينيا، أطلق عليه اسم "وحدة مبادرات جرائم الإنترنت ودمج مواردها" (CIRFU). ويقوم محللو هذه الوحدة بإلغاء مسارات التحقيق الخاطئة ويغربلون أدلة القضية وينفقونها قبل إحالتها إلى وكالات تطبيق القوانين أو فرق العمل الخاصة المحلية أو الدولية.

تحظي وحدة مبادرات جرائم الإنترنت (CIRFU) بالدعم من بعض أكبر الشركات التي يستهدفها مجرمو الفضاء السبراني، أي المنظمات والتجارة الذين يعملون في مجال الإنترنت مثل مايكروسوفت، وإي باي/باي بال، وأميركا أونلاين، وجمعيات هذه الصناعة التجارية مثل اتحاد برامج كمبيوتر الأعمال، وجمعية التسويق المباشر، ومجلس مخاطر التجار، وصناعة الخدمات المالية، وغيرها. وقد انضم محققون ومحللون من هذه المنظمات، يعمل الكثير منهم على قضايا جرائم الإنترنت، إلى وحدة المبادرات المذكورة لتحديد اتجاهات وتكنولوجيات وجرائم الإنترنت، ولجمع

المعلومات لإعداد ملفات قضايا قانونية ذات شأن، ولمساعدة وكالات تطبيق القانون في جميع أنحاء العالم علي اكتشاف جرائم الإنترنت ومحاربتها.

ويستعاون في وحدة المبادرات موظفون فيدراليون ومحللون من القطاع الأكاديمي وقطاع صناعة الإنترنت سوية للتوصل إلي معرفة المصدر الذي تنبثق عنه الجريمة، ومن يقف وراءها، وطريقة محاربتها، وعندما تسمع وحدة المبادرات من مجموعة صناعية عن اتجاه أو مشكلة معينة، تشكل الوحدة مبادرة لاستهداف بعض كبار المجرمين وإلقاء القبض عليهم، ولا تكتفي بمقاضاتهم بل تسعى لمعرفة المزيد عن كيفية قيامهم بعملياتهم. وعقب ذلك، يبلغ مكتب الشكاوي الجمهور عن هذه الاتجاهات وعن العمليات الاحتمالية وذلك من خلال إصدار بيان خدمة عامة ينبه الشعب وينشر علي موقع مكتب الشكاوي أو يوزع بطرق أخرى.

واستنادا إلي معطيات شكاوي المستهلكين أو قطاع صناعة الإنترنت، يرصد المحققون الاتجاهات والمشاكل ويضعون بالتعاون مع شركاء في صناعة الإنترنت مبادرات لفترة تمتد ما بين ستة أشهر وسنة لاستهداف النشاطات الإجرامية، بما في ذلك ما يلي:

\* **إعادة الشحن:** عملية يتم من خلالها توظيف متآمرين أو شركاء لا علم لهم بالموضوع، في الولايات المتحدة، لاستلام طرود تحتوي علي بضائع إلكترونية، أو سلع أخرى، كان قد تم شراؤها بواسطة بطاقات ائتمان مزورة أو مسروقة، فيعاد توصيلها وشحنها، عادة إلي خارج البلاد، وعندما يكشف التاجر أن بطاقة الائتمان كانت مزورة، تكون البضاعة قد أصبحت في بلد آخر.

\* **البريد الإغراقي الإجرامي:** وهو عبارة عن رسائل إلكترونية أن تكون قد طلبت وتستعمل للاحتيال علي المؤسسات المالية، وتزوير بطاقات الائتمان وسرقة الهوية، والجرائم الأخرى. ويمكن أن يستعمل البريد الإغراقي أيضا

كوسيلة للدخول إلى الكمبيوترات الخاصة وأجهزة شركات تقديم خدمات الإنترنت دون إذن، أو لإيصال الفيروسات وبرمجيات الكمبيوتر الإجرامية إلى كمبيوترات أخرى.

\* اصطيد كلمات المرور: وهو محاولات لسرقة كلمات السر الإلكترونية والمعلومات المالية عن طريق تظاهر المحرم بأنه شخص جدير بالثقة أو مؤسسة أعمال عبر اتصال إلكتروني يبدو وكأنه رسمي، كرسالة إلكترونية أو موقع إلكتروني.

\* سرقة الهوية: هي نتيجة عمل يقوم به المجرم مستخدماً معلومات شخصية مسروقة لشخص ما من أجل اقتراض عملية احتيال أو جرائم أخرى. وكل ما يحتاجه المجرم لسرقة هوية هو القليل من المعلومات الشخصية.

#### التواصل الدولي:

يعمل مركز الشكاوي الخاصة بجرائم الإنترنت أيضاً مع منظمات دولية مثل هيئة الجرائم الاقتصادية والمالية (EFCC) في نيجيريا، حيث توجد مستويات عالية من الجرائم الاقتصادية والمالية كتهريب الأموال والاحتيال بقبض أموال مسبقة لمشاريع وهمية، أو ما يسمى احتيال ٤١٩، مما كانت له عواقب سلبية شديدة على ذلك البلد.

وتجمع جريمة احتيال ٤١٩، التي أطلق عليها اسمها لخرقها الفقرة ٤١٩ من مدونة القوانين الجنائية النيجيرية، ما بين جرم انتحال الشخصية وتشكيكة متنوعة من مؤتمرات قبض الأموال مسبقاً لمشاريع وهمية، فالضحية المحتملة تتلقى رسالة، أو رسالة إلكترونية، أو فاكس، من أشخاص يدعون أنهم موظفون حكوميون نيجيريون أو أجانب، يطلبون فيها المساعدة في إيداع مبالغ طائلة من المال في حسابات في مصارف خارجية، عارضين حصة من الأعمال مقابل ذلك. ويعتمد المخطط على إقناع الضحية الراغبة في

التعاون بإرسال مبلغ من المال إلي كاتب الرسالة علي دفعات لأسباب متنوعة.

وقد أدي خطر هذه الجرائم في نيجيريا إلي تأسيس لجنة الجرائم الاقتصادية والمالية هناك. وخلال السنة ونيف الماضية، قام مركز الشكاوي الخاصة بجرائم الإنترنت بعدة عمليات جديدة صودرت فيها بضائع وتم إلقاء القبض علي أشخاص في أفريقيا الغربية نتيجة لهذا التحالف بين المركز ولجنة الجرائم الاقتصادية والمالية، ونتيجة لتحالفات أخرى.

ويعمل مركز الشكاوي عن كثب أيضا مع المنظمة الكندية المسماة "الإبلاغ عن الجرائم الاقتصادية علي خط الإنترنت" (RECOL). ويدير هذه المنظمة المركز القومي للجرائم المكتبية في كندا، وتدعمها شرطة الخيالة الملكية الكندية، ووكالات أخرى. وتتطوي منظمة الإبلاغ عن جرائم الإنترنت علي شراكة متكاملة بين وكالات تطبيق القوانين الدولية والفيدرالية والإقليمية من جهة، وبني المسؤولين عن وضع وتطبيق أنظمة العمل والمنظمات التجارية الخاصة التي لها مصلحة تحقيقية مشروعة في تلقي شكاوي الجرائم الاقتصادية، من جهة أخرى.

وهناك مجموعة متنامية من الوكالات الدولية المنخرطة في محاربة جرائم الإنترنت. ويعمل مركز الشكاوي الخاصة بجرائم الإنترنت مع المسؤولين عن تطبيق القانون في بلدان عديدة، بينها استراليا والمملكة المتحدة. كما يحضر ممثلو مركز الشكاوي أيضا اجتماعات دورية للمجموعة الفرعية حول جرائم التكنولوجيا المتقدمة التابعة لمجموعة الثماني (كندا، فرنسا، ألمانيا، إيطاليا، اليابان، روسيا والمملكة المتحدة والولايات المتحدة). ويعمل قسم من هذه المجموعة الفرعية علي محاربة جرائم الإنترنت وتعزيز التحقيقات بشأنها.

ومشروعاً مركز الشكاوي الخاصة بجرائم الإنترنت (IC3)، ووحدة مبادرات جرائم الإنترنت ودمج مواردها (CIRFU)، هما بمثابة عمل متطور ومستقدم باستمرار. وأثناء هذا التقدم، يراجع موظفو ومحللو مركز الشكاوي ما أثبت نجاحه وما ثبت فشله من إجراءات، ويسعون باستمرار لتأمين مساعدة الخبراء والمصادرة التي تزودهم بمعلومات استخباراتية ليصبحوا أكثر فطنة بخصوص جرائم الإنترنت، ولكي يتعلموا كيف يمكنهم محاربتها بصورة أكثر فعالية. فهذه هي مهمة مركز الشكاوي الدائمة التي لا تتغير.

#### الجريمة البلاستيكية أخطر جرائم بطاقات الائتمان: (١)

الجريمة البلاستيكية جريمة معلوماتية خطورتها تكمن في أنها بوابة المرور لغاسلي الأموال القذرة، وأقطاب المخدرات والمجرمين الذين يمكنهم من خلال ما تقدمه الجريمة البلاستيكية أن يمارسوا أنشطتهم وتحويلاتهم الحالية في خفاء شرعي وأن كان جرماً ولما كانت الجرائم البلاستيكية من الجرائم المستحدثة الناشئة عن استخدام واستغلال التكنولوجيا الحديثة. فقد أصبحت من الأمور الضرورية البحث عن التكيف للصور المختلفة لجرائم بطاقات الائتمان.

أولاً: عملية تزوير بطاقات الائتمان وإشعاراتهم تستلزم بحث الأحكام العامة لجريمة التزوير في المحررات ذلك لأن بطاقات الائتمان ما هي إلا بيانات خاصة مرئية وغير مرئية معالجة إلكترونيا وكذلك إشعاراتها ما هي إلا محورات صادرة من البنوك ويقوم حامل البطاقة بالتوقيع على تلك الإشعارات في عمليات السحب أو الإيداع النقدي.

---

(1) د. معتز محيي عبد الحميد.

المركز الجمهوري للبحوث والدراسات الأمنية:

ثانياً: لا شك أن البيانات المرئية علي بطاقة الائتمان تتوفر فيها مقومات المحرر أما بالنسبة للبيانات غير المرئية والمعالجة إلكترونياً علي البطاقة فإن عملية تغييرها تدفعنا تساؤل مهم، هل يمكن القول بأن التغيير وقع علي محرر؟ الإجابة هنا نجدها في اتجاه جانب من الفقه في شرح قانون العقوبات إلي أن فكرة المحرر تفترض أن دلالة الرموز التي تستشف بالنظر إليها أي أن حاسة البصر هي التي تكشف الفقرة التي يعبر عنها المحرر وبالتالي فإنه لا يعد محرراً ما تم تسجيله من بيانات غير مرتبة ومعالجة إلكترونياً أي كانت الأهمية القانونية لما تم تسجيله فالتزوير يفترض تغييراً في علامات أو رموز مرئية ويرى جانب آخر من الفقه القانوني توافر فكرة المحرر في البيانات غير المرئية والمعالجة إلكترونياً وبالتالي تتحقق جريمة التزوير إذا حدث تغيير في المحرر وتوافرت بقية أركان التزوير.

ثالثاً: استصدار بطاقات ائتمان صحيحة بمستندات مزورة مثل البطاقة الشخصية أو جواز السفر أو شهادة الجنسية أو خطاب موجه من الجهة التي يعمل بها ببيانات غير سليمة وأختام مزورة، هنا تنطبق علي هذه الحالة الأحكام العامة للتزوير واستعمال المحررات المزورة.

بعد هذا العرض لابد من أن نضع صورا تقي الجميع خطورة الجريمة البلاستيكية ونجد هذا في ضرورة اتباع الآتي<sup>(١)</sup>:

١- تغيير نظام الشراء عن طريق الإنترنت وعدم الاكتفاء برقم البطاقة الائتمانية فقط بل يجب أن تكون هناك مطالب أخرى مثل ضرورة أن تطلب بيانات عن العميل كرقم تحقيق الشخصية والعنوان والتوقيع المعتمد في البطاقة ويجب إدخال رقم (كودي) خاص بالعميل حتى لا يستغل النقاط أرقام

(1) <http://www.2alsaha.Com/paper.Php?Source=akbar&ml>

بطاقات ائتمان لبعض العملاء من الشبكة وإعادة التعامل بها دون علم أصحابها.

٢- إنشاء قاعدة بيانات تتضمن معلومات كافية عن قضايا بطاقات الائتمان في الداخل والخارج، وأحدث أساليب المواجهة لهذه الجرائم من خلال التنسيق والتعاون مع المنظمات العالمية التي تستعمل (الفيزا والماستر كارد) للاستفادة من الخبرة في هذا المجال.

٣- التفتيش الدوري علي ماكينات البيع الإلكترونية بواسطة متخصصين لكشف أي تلاعب في نظم تشغيلها.

٤- ضرورة توفير أجهزة الكشف بالأشعة فوق البنفسجية لدى موظفي البنوك المتخصصة لبطاقات الائتمان.

٥- يجب تغيير رقم بطاقة الائتمان لحاملها كل عام حتى لا يستغل نفس الرقم في البطاقات المنتهية الصلاحية بتغيير رقم بطاقة الائتمان لحاملها كل عام حتى لا يستغل نفس الرقم في البطاقات المنتهية الصلاحية بتغيير البيانات بآلة تشفير البيانات علي الشريط المغنط من الرصيد وتواريخ السحب وخلافه.

٦- زيادة الدورات التدريبية المتخصصة لموظفي البنوك العاملين في مجال بطاقات الائتمان الإلكترونية للتعرف علي طرق الكشف عن تزوير البطاقات الخاصة بتحقيق الشخصية والأختام والمستندات والأوراق المستخدمة في استجواب بطاقة الائتمان.

أما بالنسبة لبطاقة الائتمان فكما نحمي حاملها من الجريمة البلاستيكية فيجب أن ندعمها بالآتي:

أ- أن يحتوي شريط التوقيع علي طباعة رقيقة بحيث لا تظهر أو تظهر بصورة مشوهة عند تزيف طباعتها بالحاسب الآلي.

ب- دمج مكونات مادة شريط التوقيع الورقية بمواد كيميائية تؤدي إلى تغيير اللون في حالة أي محو آلي أو كيميائي.

ج- استخدام أختام ضاغطة وأحبار مؤمنة غير مرئية على الصورة.

د- وضع أحبار قلووية مؤمنة وغير مرئية تعطي توهجا تحت الأشعة دون البنفسجية في شريطك التوقيع التعاون الأمني في مكافحة الجريمة البلاستيكية.

هنا تبرز أهمية التعاون الإقليمي والدولي بين الأجهزة الأمنية في قضايا وجرائم بطاقات الائتمان بغرض تبادل المعلومات والخبرات من خلال المكاتب الإقليمية والدولية المتخصصة وأخيرا أن الجريمة البلاستيكية هي جريمة خطيرة تسبب إليها المجتمع الدولي في القرن الماضي وتحديدا في مؤتمر الأنتربول الثامن الذي عقد في أوتاوا بكندا سنة ١٩٩٢ وأشار المؤتمر إلى تعاظم تلك الجريمة التي أصبحت إحدى الظواهر الإجرامية العامة على المستوى الدولي، الأمر الذي بات يحتم علينا أن ننتبه إلى ضرورة التصدي العلمي وإلقاء الضوء على الصور المختلفة لتلك الجريمة بحثا عن الأمثل في طرق المواجهة والفحص واشتقاق الدليل المادي لهذه الجريمة حماية لكل مناحي الاقتصاد عن محاولات اختراقه عبر الجريمة المنظمة<sup>(١)</sup>.

جرائم التجسس والإرهاب الإلكتروني عبر الإنترنت<sup>(٢)</sup>:

إن شبكة الإنترنت كشبكة معلوماتية تنطبق عليها النموذج المعروف لها من المعلومات ذو الأبعاد الثلاثة وهي:

١- سرية المعلومات: وذلك يعني ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات أو المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المحولين لذلك.

(١) شبكة الإعلام العراقي.

(٢) محمد محمد الألفي.



٢- سلامة المعلومات: يتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة على أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المحولين لذلك.

٣- وجود المعلومات: وذلك يتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسب إلا من قبل الأشخاص المحولين لذلك. إن جرائم الإنترنت ليست محصورة في هذا النموذج بل ظهرت جرائم لها صور أخرى متعددة تختلف باختلاف الهدف المباشر في الجريمة.

إن أهم الأهداف المقصودة في تلك الجرائم هي كالآتي<sup>(١)</sup>:

١- المعلومات: يشمل ذلك سرقة أو تغيير أو حذف المعلومات، ويرتبط هذا الهدف بشكل مباشر بالنموذج الذي سبق ذكره.

٢- الأجهزة: ويتمثل ذلك تعطيلها أو تخريبها.

٣- الأشخاص أو الجهات: تهدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد والابتزاز.

علماً بأن الجرائم التي تكون هدفها المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلى الأشخاص المعينة أو الجهات المعنية بتلك المعلومات أو الأجهزة<sup>(٢)</sup>.

هذا وإن كانت هناك وسائل لحماية الخصوصية أثناء تصفح الإنترنت إلا أنه من الصعب جداً على السيطرة ما يحدث بالمعلومات بمجرد خروجها من جهاز الحاسب وعلى ذلك فإن حماية الخصوصية يجب أن تبدأ من البداية لتحديد نوعية البيانات التي لا ينبغي أن تصبح عامة ومشاعة ثم تتغير الوصول إلى تلك المعلومات جرائم التجسس الإلكتروني.

(1) <http://www.arab2000.net/wnewsDetails.asp?Id=29306&cid=56>.

(2) محمد محمد الألفي.

ففي عصر المعلومات وبفعل وجود تقنيات عالية التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبعث الفضائي، ولقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرف الإلكترونية خاصة مع استخدام الإنترنت وانتشاره عالميا.

ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة HACKERS فمخاطر هؤلاء محدودة وتقتصر غالبا على العبث أو إتلاف المحتويات والتي يمكن التغلب عليها باستعارة نسخة أخرى مخزنة، أما الخطر الحقيقي فيكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخبارية للحصول على أسرار ومعلومات الدولة ومن ثم إفشائها لدولة أخرى تكون عادة معادية، أو استغلالها بما يضر المصلحة الوطنية للدولة.

وقد وجدت بعض حالات التجسس الدولي ومنها ما اكتشف أخيرا عن مفتاح وكالة الأمن القومي الأمريكي NSA والتي قامت ببراءته في نظام التشغيل الشهير وندوز، كما كشف أخيرا النقاب عن شبكة دولية ضخمة للتجسس الإلكتروني تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كندا وبريطانيا وأستراليا ونيوزيلندا، لرصد المكالمات الهاتفية والرسائل بكافة أنواعها ويطلق عليها اسم (ECHELON).

فمع توسع التجارة الإلكترونية عبر شبكة الإنترنت تحولت الكثير من مصادر المعلومات إلى أهداف للتجسس التجاري، ففي تقرير صدر عن وزارة التجارة والصناعة البريطانية أشار إلى زيادة نسبة التجسس على الشركات من ٣٦% عام ١٩٩٤ إلى ٤٥% عام ١٩٩٩، كما أظهر استفتاء أجري عام ١٩٩٦ لمسئولي الأمن الصناعي في الشركات الأمريكية عن حصول الكثير من الدول وبشكل غير مشروع على معلومات سرية لأنشطة

تجارية وصناعية في الولايات المتحدة الأمريكية. وبعد الاعتداءات الأخيرة على الولايات المتحدة الأمريكية صدرت تعليمات جديدة لأقمار التجسس الاصطناعية الأمريكية بالتركيز على أفغانستان والبحث عن الجماعات المعادية لها، وقررت السلطات الأمريكية للاستعانة في عمليات التجسس على أفغانستان بقمريين اصطناعيين عسكريين مصممان خصيصا لالتقاط الاتصالات التي تجري عبر أجهزة اللاسلكي والهاتف المحمولة بالإضافة لقمريين اصطناعيين آخرين يلتقطان صوراً فائقة الدقة، وفي نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاستعانة بقمريين تابعين لهما لرصد الاتصالات ومن ثم تحول بعد ذلك إلى الولايات المتحدة حيث تدخل في أجهزة كمبيوتر متطورة لتحليلها.

#### جرائم الإرهاب الإلكتروني:

في عصر الازدهار الإلكتروني وفي زمن قيام حكومات إلكترونية، تبدل نمط الحياة وتغيرت معه الأشكال الأشياء وأنماطها ومنها ولا شك أنماط الجريمة والتي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها والقديمة في اسمها جريمة الإرهاب الإلكتروني والتي أخذت أشكال حديثة تتماشى مع التطور التقني، ويتغير وتطور الأساليب التي يحاول المفسدين الوصول بها إلى أهدافها فقد غدي الإرهاب الإلكتروني هو السائد حالياً.

وأصبح اقتحام المواقع وتدميرها وتغييرها محتوياتها والدخول على الشبكات والعبث بمحتوياتها بإزالتها أو بالاستيلاء عليها أو الدخول على شبكات الاتصالات أو شبكات المعلومات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائياً أصبح هو أسلوب الإرهاب حالياً في محاولة الوصول إلى أغراضها.

وفي إحدى الوقائع، حيث قام مجهول باقتحام شبكة اتصالات شركة لخدمات الكمبيوتر والإنترنت وإنتاج البرامج، والذي أدى إلى تعديل جميع اتصالات الشبكة مما أدى إلى تلف الشبكة والأجهزة، وتكبدها خسائر مالية جسيمة، بالإضافة لما ترتب عن ذلك من أضرار معنوية وأدبية، وتبين أن مرتكب الواقعة هو المسئول عن الشركة المنافسة في ذات المجال والهدف من ذلك هو إلحاق الضرر بالشركة المجني عليها المنافسة ولوجود خلافات سابقة إبان عمله بالشركة الأولى.

#### جرائم الإنترنت قوا أبناءكم ناراها<sup>(1)</sup>:

في ظل التطورات الهائلة لتكنولوجيا المعلومات، واستحداث شبكة<sup>(2)</sup> المعلومات الدولية التي تربط العالم في قرية إلكترونية واحدة، ونظرا للعدد الهائل من الأفراد والمؤسسات الذين يرتادون هذه الشبكة فقد أصبح من السهل ارتكاب أبشع الجرائم بحث مرتاديه سواء كانوا أفرادا أم مؤسسات أم مجتمعات محافظة بأكملها.

لقد امتدت أشكال ارتكاب الجريمة إلى الإنترنت حيث أصبحت أسهل الوسائل أمام مرتكبي الجريمة، فراح المجرمين ينتهكون الأعراض، ويغترون بالأطفال، إضافة إلى اقترافهم لجرائم التشهير وتشويه السمعة عبر مواقع إلكترونية مخصصة لهذا الهدف، ولم ينته بهم الأمر إلى هذا الحد بل راحوا ينتحلون شخصيات أناس معينين وخاصة في المؤسسات التجارية فينصبون ويحتالون ومن ثم يتلشون كالسراب في الصحراء.

(1) / ميرفت عوف.

(2) <http://www.lahaonline.com/index.php?option=content&id=8989&task=view&sectionid=1>

"لها أون لاين" تعرض صوراً من الجرائم التي تقترب بواسطة شبكة المعلومات الدولية الإنترنت وتتحدث لمتخصصين في كيفية حماية الأسرة من هذه الجرائم:

حين دشنت شبكة المعلومات الدولية الإنترنت كانت تتمتع بقدر من الأمان والسرية في تبادل المعلومات، لكن الحال لم يدم طويلاً حيث اتسعت دائرة مستخدمي الإنترنت فلم تعد مقتصرة فقط على الباحثين والمنتسبين للجامعات، وأصبحت تضم أجيالاً مختلفة وثقافات متفاوتة كما أن أساليب الاستخدام تنوعت وتعددت أشكالها، فبين الدردشة وتصفح المواقع الترفيهية والثقافية والمتخصصة بكافة ألوانها وأطيافها، وليس انتهاء باستخدام الإنترنت كوسيلة لترويج المنتجات وتسويقها...

ثم جاء مجرمي الإنترنت لانتحال الشخصيات والتغريب بصغار السن بل تعدت جرائمهم إلى التشهير وتشويه سمعة ضحاياهم الذين عادة ما يكونوا أفراداً أو مؤسسات تجارية ولكن الأغرب من ذلك أنهم يحاولون تشويه سمعة مجتمعات بأكملها خاصة المجتمعات الإسلامية، وهذا ما حد بالعالم لتحرك فقبل عدة شهور وقعت ٣٠ دولة على الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في العاصمة المجرية بودابست، وشملت المعاهدة عدة جوانب من جرائم الإنترنت، بينها الارهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.

الاتفاقية التي أظهرت مدى القلق العالمي من جرائم الإنترنت اصطدمت بتارين أولهما حكومي طالبت به أجهزة الشرطة وهو الرقابة الصارمة على مستخدمي الإنترنت والسيار الثاني رفض المنظمات المدافعة عن حقوق الإنسان، والصناعات المعنية ومزودي خدمات الإنترنت للحد من حرية الأفراد في استخدام الإنترنت.

#### جرائم وأهداف متعددة: (١)

ويعرض د. إلياس الهاجري في أهم البحوث التي تناولت جرائم الانترنت لأنواع معينة من الجرائم منها استهداف فئة كبيرة من الجرائم على شبكة الانترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز، حيث يقوم المجرمون بسرقة أجهزة الحاسب المرتبطة بالانترنت أو تدميرها مباشرة أو تدمير وسائل الاتصال كالأسلاك والأطباق الفضائية وغيرها، ويوضح د. الهاجري أن صناعة ونشر الفيروسات أيضا من أكثر جرائم الانترنت انتشارا وتأثيرا، كما أن الاختراقات تتم من خلال برامج متوفرة على الانترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير.

ويشير د. الهاجري (٢) إلى وجود جرائم الإنترنت تستهدف جهات سواء كانوا أفرادا أو مؤسسات، فمثال جرائم انتحال الشخصية: هي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات، وتتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أى هوية الضحية) أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى، ويتطرق د. الهاجري إلى جرائم المضايقة والملاحقة التي تتم باستخدام البريد الإلكتروني أو وسائل الحوارات الآتية المختلفة على الشبكة، وتشمل الملاحقة رسائل تهديد وتخويف ومضايقة ويؤكد الباحث أن كون طبيعة جريمة الملاحقة على شبكة الانترنت لا تتطلب اتصال مادي بين المجرم والضحية لا يعني بأي حال من الأحوال قلة خطورتها، ففترة المجرم على إخفاء هويته تساعده على التمداد في جريمته

(1) <http://www.lahaonline.com/index.php?option=content&id=8989&task=view&sectionid=1>

(2) د. إلياس الهاجري.

والسنى قد تقضي به إلى تصرفات عنف مادية علاوة على الآثار السلبية النفسية على الضحية.

أما جرائم التفرير والاستدراج فإن أغلب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمى الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم فى تكوين علاقة صداقة على الانترنت والتي قد تتطور إلى التقاء مادي بين الطرفين - أما فيما يتعلق بالتشهير وتشويه السمعة فإن المجرم يقوم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فرداً أو مجتمع أو دين أو مؤسسة تجارية أو سياسية، وتعد خطيرة هذه الجرائم أيضا كما يذكر د. الهاجرى صناعة ونشر الإباحية حيث جعل الانترنت الإباحية بشتي وسائل عرضها من صور وفيديو وحوارات فى متناول الجميع، ومن السهل هنا بتفريز الأطفال فى أعمال إباحية أو نشر مواقع تعرض مشاهدة إباحية لأطفال.

#### آليات الحماية:

بإشارة إلى الاتفاقية الدولية السابقة تضح مدى صعوبة التحكم فى حماية مستخدمى الانترنت من مجرميه، وهذا ما يؤكد المهندس وليد كساب مدير عام شركة Pis ل' لها أون لاين" فيقول: " هذه مزايا التكنولوجيا تنشر العلم والمعرفة والمعلومات بإيجابيتها وسلبيتها بشكل رهيب، وكون هذه المعلومات وسيلة انتشار جيدة للكثير فهو مفتوحة على الإيجابي والسلبي " ويضيف: " جرائم الانترنت لها علاقة بشكل أولى بالمواقع الجنسية، لكن هناك خدمات تتوفر لمنع هذا الجرائم يتحكم بها رب الأسرة بالدرجة الأولى وهى عبارة عن انترنت "فلتر" ، توفها شركات خاصة" وقال: " يجب أن يكون رب الأسرة متأكد من أن خط الانترنت الموصول بجهاز منزله به "فلتر" يمنع وصول هذه المواقع لأيدى أطفاله أو أفراد أسرته" ، أما فيما يتعلق بالشات

كون وسيلة متاحة يستخدمها الجميع فى أمور إيجابية كثيرة كمخاطبة الأهل والأصدقاء والأقارب المغتربين كوسيلة أوفر وأرخص ووسيلة قد يصل مجرمى الانترنت عن طريقها لتغيير بأحد ما قال: " هنا يلعب دور التحكم من البيت وزرع الثقة بالأبناء الدور الرئيسى"، ويؤكد كساب أن الاتفاقيات الدولية التى وقعت بخصوص جرائم الانترنت من الصعب تطبيق ما نتج عنها داخل المجتمعات لأن الانترنت مفتوح فى أى مكان ويمكن الحصول على معلومة فى أى وقت، ووجه كساب نصيحة لرب الأسرة قائلا: " الشئ المفيد فى هذا المجال أن يكون تحكم من العائلة وهذه رئيسية وعليها أن تتحكم بماذا يرى الأطفال وماذا لا يرون وأنصح رب الأسرة أن يكون متأكد من وجود فلتز لهذا الانترنت، وعليه أن ينقى خدمة من شركة يوجد بها خدمة لتصالات المشتركين لمتابعة تحركات ابنه على الانترنت لادى خروجه من البيت".

نفسيا يؤكد لنا د. خالد دحلان الخبير النفسى فى برنامج غزة للصحة النفسية أن تعرض أحد أفراد الأسرة لإحدى جرائم الانترنت يخلق نوع من الاحباط والقلق الشديد ومزيد من الاكتئاب يعم عليه حتى لو كانت الجريمة غير مادية، فمجرد تحرش لفظي يسبب إيذاء للضحية"، ويصر دحلان على أن التنشئة الاجتماعية وزرع الثقة فى أفراد الأسرة أهم من كل الاحتياطات المادية التى قد تفشل فى منع وصول لأحد أفراد الأسرة أما إذا كانت التنشئة فيها شئ من الخلل والشخصية مشوهة والنفسية معتلة سيبحث هو عن مجرمي الانترنت، وأضاف: " يجب أن نعود أولادنا على العفة والطهارة وحفظ الذات، وهذا هو الأساس فى حفظهم من مجرمي الانترنت".

#### جحا وجرائم متواصلة:

وبعد أن تعرفنا على جرائم الانترنت أثرتنا أن نحدث بعضا من الذين تعرضوا لمثل هذه الجرائم التقينا الفنانة الكاركتير المعروفة أمية جحا



والتي أكدت أنها تعرضت مباشرة بعد أحداث الحادى عشر من سبتمبر والتي انطوى عليها تدمير البرجين، سألتها عن نوعية الجريمة فقالت: " كانت مضايقة وملاحقة وتهديد بالقتل وتخويف، أنا أعرف الجهة التي هددتني فقد عرفتني بشخصها وبنيتها الصديقة في التلخص"، وكان السبب رسماً كاريكاتيرياً يصور الأمة العربية والتي رمزت لها أمية بأمرة تلبس الثوب العربي وتنظر للبرجين وترغد بفرحة واضحة على ملامح وجهها الذي أعياه طول انتظار لحظة النصر، وتتابع أمية: " وضعت هذا الرسم على الموقع الإلكتروني الخاص بي لخمس دقائق وما هي لحظات حتى انتهت على رسائل التهديد والتخويف لكنني لم أكرث كثيراً بها...

لست وحدها الفنانة أمية من تعرضت لجرائم الانترنت فهذه الشابة أمل ذات السبعة عشر ربيعاً تحدثنا عن مأساتها مع الانترنت تقول: " في بداية الأمر كنت أستخدم الانترنت لإنجاز الأبحاث العلمية التي يكلفنا بها المدرسين، قلت جيد أن نستخدم تكنولوجيا المعلومات للاستفادة العملية"، تحمر وجنتاها وتتنظر إلى بخجل ثم تقول: " لم يكن استخدامي للانترنت فقط للأبحاث العلمية بل أنني كنت أملك بريداً إلكترونياً استقبل خلاله رسائل الأهل في الخارج كنوع من التواصل ولكن في إحدى المرات فوجئت بشخص يريدني أن أضيفه لدى قائمة المحادثة الفورية حسبته أحد أقرائي فأضفته ولكن منذ المحادثة الأولى أيقنت أنه ليس كذلك فأخذ يتحدث إلي بأسلوب مهذب يطلب صدقتي فقبلت ورحت أتحدث إليه وبعد فترة بدأ يطلب صورتي لترداد معرفتنا ببعض وبكل سذاجة بل غباء أرسلت له بالصورة وهنا كانت الكارثة حيث وجدت صورتي تنتقل من شخص لآخر وضعت بعدها...

كانت تلك نموذجاً حياً لجريمة التغيرير والاستخراج لتلك الشابة اليناعة وانطوى عليها جريمة أبشع حيث استغل المجرم صورتها للتشهير بها وتشويه سمعتها...

## جرائم الانترنت تتفاقم فى عام ٢٠٠٤<sup>(١)</sup>

شهد عام ٢٠٠٤ تزايداً هائلاً فى التهديدات الأمنية التى تستهدف أجهزة الكمبيوتر التى تستخدم برامج تشغيل ويندوز<sup>(٢)</sup>.

وتجاوز عدد الفيروسات المعروفة المئة ألف فيروس بحيث ارتفع عدد الفيروسات الجديدة بنسبة خمسين بالمئة.

كما سجلت محاولات النصب فى الانترنت- والتى يحاول من خلالها بعض المحتالين خداع الناس لمعرفة معلومات سرية- زيادة بنسبة أكثر من ٣٠ بالمئة، وأصبحت الهجمات الإلكترونية أكثر تعقيداً.

وقال كيفين هوجن، مدير كبير فى مجموعة سيمنتيك لمكافحة الفيروسات إن عام ٢٠٠٤ شهد انحساراً فى تأثير القراصنة المراهقين الذين يريدون الوصول للشهرة عن طريق كتابة فيروسات سريعة الانتشار.

ورغم استمرار هؤلاء المراهقين فى كتابة عبارات مشفرة مضرّة، شهد عام ٢٠٠٤ ارتفاعاً كبيراً فى استخدام البرامج بشكل غير قانوني.

وقال هوجن إن الحافز المادى هو ما يقود إلى هذا الاستخدام غير الشرعي لهذه التكنولوجيا.

وقد أبدى فى هذا الرأى ، جراهام كلولي، مستشار كبير فى شركة سوفوس لمكافحة الفيروسات.

ويقول كلولي: "عندما تتدخل المطاعم التجارية، يصبح كل شئ مباح، ويبحث حينها القراصنة عن تحقيق أكبر كم من الأموال".

(1) <http://news.bb.co.uk/hi/arabic/sci-tech/newsid-4134000/4134021.stm>

(2) مارك وورد  
مراسل بي بي سي للشؤون التقنية

كما ازداد عدد عمليات النصب عن طريق الانترنت والتي يحاول خلالها القراصنة إقامة مواقع بنوك مزورة، وإقناع المودعين بتسليم أرقامهم البنكية السرية، خلال هذا العام.

ورصدت دورية الشبكة الخاصة بشركة لايكوس أوروبا زيادة قدرها ٥٠٠ بالمئة في عدد رسائل البريد الإلكتروني الخادعة.

ورصدت جماعات مقاومة النصب على الإنترنت زيادة في عدد الهجمات التي تستهدف مواقع جديدة بنسبة ثلاثين بالمئة أو أكثر في الشهر.

ويجد من يقعون في فخ هذه العمليات أن حساباتهم البنكية قد تم إفراغها من محتواها أو أن سمعتهم قد تم تدميرها من خلال انتحال آخرين لها.

وقد يعني التغيير في مستويات كتاب الفيروسات زوال الفيروس الذي يرسل إلى آلاف العناوين الإلكترونية والذي تسعى للانتشار من خلال خداع الناس لفتح محتويات رسائل تشتمل على فيروس.

#### **التحكم عن بعد:**

**ويقول هوجن** إن كتاب برامج دودة الكمبيوتر أصبحوا أكثر اهتماما بجلب أجهزة كمبيوتر للاشتراك فيما يسمى ، بالبووت نيت، وهي شبكات كمبيوتر يتم التحكم فيها عن بعد ويستخدمها قراصنة الانترنت في شن هجمات على مواقع الانترنت.

وأصدرت مجموعة، سيمانتيك، تقريرا في سبتمبر/ أيلول رصدت فيه زيادة أعداد الكمبيوترات المساهمة في البوت نيت من ٢٠٠٠ إلى ٣٠٠٠٠ في الوقت الراهن.

وبسبب شبكات البوت نيت بقيت مشكلة رسائل البريد الخادعة موجودة في عام ٢٠٠٤، وقد رصدت شركات مناهضة للفيروس المكتسح تقلص نسبة

البريد الإلكتروني القانوني في بعض الأحيان إلى ٣٠ بالمئة من إجمال الرسائل.

ويرجع الخبراء انتشار شبكات البوت نيت إلى الاختلاف الكبير في الأساليب التي يتم من خلالها تكوين هذه البرامج.

ففي برامج الفيروسات التقليدية مثل نيتسكي يكتبها شخص واحد فقط. إلا أن برامج مثل جاويوت أو سباي بوت، مخالفة للأولي، يعرف الكثيرون عباراتها السرية المشفرة، ويشترون معا في صنع تنويعات على العبارة السرية الأصلية في نفس الوقت.

والنتيجة النهائية أنه يوجد أكثر من ٣٠٠٠ نوع مختلف من دودة سباي بوت.

#### الهدف المتحرك:

وقد شهد عام ٢٠٠٤ ظهور أول فيروس خاص بأجهزة الهاتف المحمول. ففي الماضي كانت التهديدات التي تستهدف الهواتف الذكية نظرية فقط لأن البرامج التي تهدد هذه الأجهزة كانت متوفرة في المختبرات وليس في الخارج.

وفي يونيو/ حزيران الماضي، اكتشف فيروس كابير الذي يمكنه الانتقال من هاتف إلى آخر باستخدام تقنية "بلوتوث" للارسال قصير المدى.

وقد أطلق في هذا العام لعبة "الموسكيتو" التي تصيب أجهزة الهاتف المحمول وتجعل الجهاز يبعث رسائل إلى قائمة الهواتف المستعملة دائما بشكل سرى، وفي نوفمبر/ تشرين الثاني، برز فيروس "سكالز ترويان" الذي يمكنه تعطيل الهاتف تماما.

وعلى الجانب الإيجابي، أعلنت شركة أمن الانترنت، إف سيكيور، الفنلندية أن عام ٢٠٠٤ كان العام الذهبي لاعتقال ومعاقبة كائني الفيروسات والقراصنة ذوى النوايا الإجرامية.

وقالت الشركة إنه تم القبض على ثمانية من كاتبي الفيروسات كما تم اعتقال وإدانة البعض من أعضاء الجماعة التي تطلق على نفسها اسم " ٢٩ أى فيراس".

وكانت أكبر عملية، القبض على المراهق الألماني، سفين جاتشين، الذي اعترف أنه كان وراء كتابة الفيروسات من صنف نيتسكي وساسر.

كما أغلق كل من موقع كاردربلايت وشادوكرو واللذين كانا يستعملان لتبادل أرقام بطاقات الائتمان المسروقة بين القراصنة.

الانترنت سبب ارتفاع جرائم الجنس ضد الأطفال: (١)

قالت منظمة خيرية معنية بشؤون الطفل إن جرائم الجنس ضد الأطفال تزايدت ١٥ مرة منذ عام ١٩٨٨ وإن الانترنت المتاح على الهواتف المحمولة قد يزيد الأمر سوءا.

وأوضح تقرير لمنظمة ناشيونال تشلدرنز هوم سابقا، والتي تحمل حاليا اسم إن سى اتش، صدر يوم الأحد أن الشبكة مسؤولة إلى حد كبير عن الارتفاع الهائل في جرائم الإباحية ضد الأطفال.

وتقول المؤسسة الخيرية إن عام ٢٠٠٢ شهد ٥٤٩ جريمة جنسية ضد الأطفال مقابل ٣٥ جريمة عام ١٩٨٨.

وتخشى المؤسسة من أن يؤدي ظهور الجيل الثالث من الهواتف المحمولة، والتي تتمتع بإمكانيات تصوير الفيديو، إلى ارتفاع تلك الجرائم بشكل أكبر.

ويساور منظمة إن سى اتش القلق من استخدام مرتكبي جرائم الجنس للجيل الثالث من الهواتف المحمولة للدخول على المواقع الإباحية للأطفال والتقاط صور لمواضع جنسية مع الأطفال وتبادل تلك الصور المسيئة.

(١) <http://nesvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/hi/arabic/sci-tech/n...>

ويستغل هؤلاء صعوبة تحديد هوياتهم على الانترنت لافتراس الأطفال، لكن الشرطة تمكنت من تعقب بعضهم حتى أجهزة الكمبيوتر الشخصية الخاصة بهم.

لكن استخدام شبكة الانترنت من خلال الهواتف المحمولة سيمثل صعوبة أكبر في تعقب المجرمين.

ويعتقد التقرير أن الأرقام الأخيرة، لعام ٢٠٠٢، سترتفع بشكل أكبر مما هى عليه عند نشر الاحصاءات الأخيرة لهذا العام، بسبب تأثير عملية أور، وهو تحقيق يجرى مع ٦٥٠٠ بريطاني متهمين بالدخول على مواقع الاباحية للأطفال باستخدام بطاقات الائتمان.

وحذر مستشار شؤون الانترنت بمؤسسة أن سى اتش، جون كار، من أن التكنولوجيا الجديدة سوف "تزيد الأمور صعوبة من جهة المنع أو الحماية".

وقال كار "تقريبا جميع قضايا سلامة الأطفال على الإنترنت الموجودة حاليا ستصبح أكثر تعقيدا عندما يصبح الانترنت فى الشارع".

جرائم الانترنت تشكل نشاطا تجاريا بقيمة مليارات الدولارات:

قال تقرير أصدرته شركة سيمانتك لصناعة برمجيات حماية الحواسيب إن الجرائم التى ترتكب عن طريق الانترنت أصبحت تشكل نشاطا تجاريا واسع النطاق.

وقال التقرير إن مواقع معينة على الشبكة الدولية تنظم مزادات لبيع التفاصيل البنكية ومعلومات تخص بطاقات الائتمان وتعرض أيضا للبيع برمجيات تمكن من القرصنة على بعض المواقع على الشبكة.

وحذر التقرير من أن القراصنة يترددون على مواقع موثوقة مثل 'ماى سبيس' و'فايسبوك' لشن هجمات على حواسيب مستخدمي هذه المواقع.

ويقول التقرير إن هذه العمليات تشكل جزءا من نشاط تجارى إجرامى يقدر حجمه بمليارات الدولارات.

وأشار إلى عدد من المواقع التى يتبادل روادها معلومات وبيانات تمكن من القرصنة على البيانات المالية وانتحال شخصية الغير.

ويقول مراسل بي بي سي لشؤون التقنية، رورى سيلان- جونز، إنه يعرض للبيع على أحد هذه المواقع معلومات للولوج إلى مواقع بنكية وبيانات انتمانية بل ومئات الملايين من عناوين البريد الإلكتروني الشخصية.

كما تعرض فى مواقع أخرى برامج تتيح بناء مواقع بنكية وهمية لخداع الغير ومن ثم الحصول على بياناتهم الخاصة.





## **الفصل الثالث**

### **جريمة الغش التجارى**

### **جريمة معلوماتية بالدرجة الأولى**



## الغش التجارى فى المجتمع الإلكتروني:

لقد اتضح من التحليل السابق مدى تعدد واختلاف أشكال الجرائم الإلكترونية بشكل قد يصعب معه حصرها، فبعضها يرتبط بالمعلومات والبيانات، وبعضها يرتبط بالأجهزة، وبعضها يرتبط بالأشخاص والأموال. وعلى الرغم من تكرار حدوث هذه الجرائم في ظل تزايد أعداد مستخدمي الإنترنت، وتنامي حجم التجارة الإلكترونية، إلا أنه حتى الآن يوجد كثير من الغموض الذي يكتنفه كيفية التعامل مع هذه الجرائم، هل هي بمثابة الاعتداء على الأشخاص، أم أنها بمثابة السرقة المادية، أن أنها أو بعض منها تخضع لنظام الغش التجاري.

أيضا يثار الكثير من الجدل حول المفهوم التقليدي للغش التجاري، ومدى انطباقه على الجرائم الإلكترونية. فالغش يعرف بأنه كل فعل من شأنه أن يغير من طبيعة أو خواص المواد أو فائدتها التي دخل عليها عمل الفاعل<sup>(١)</sup>. كما يعرف بأنه كل فعل عمدي، ينال سلعة ما بتغيير خواصها أو ذاتيتها أو صفاتها الجوهرية وبشكل عام العناصر الداخلة في تركيبها، بحيث يندفع المتعاقدين الآخر، ويسهل التعرف على الغش في الحالات ذات الطبيعة المادية أو المرئية، مثل بيع اللحوم الفاسدة، بيع الأدوية المسممة، خلط البنزين بالكيروسين، بيع قطع غيار السيارات والآلات المقلدة، بيع مواد التجميل ومساحيق الوجه المنتهية الصلاحية، وغيرها. ولكن في حالات الجرائم الإلكترونية قد لا تتوافر تلك الطبيعة المادية أو المرئية بسهولة.

---

(١) عبد الفتاح بيومي حجازي، (٢٠٠٤)، "حماية المستهلك من الغش التجاري والتقليد في عقود التجارة الإلكترونية عبر الإنترنت" الندوة الثالثة لمكافحة الغش التجاري والتقليد في دول مجلس التعاون لدول الخليج العربية، الرياض، سبتمبر.  
- المصدر - دراسة أعدتها قطاع البحوث بالغرفة التجارية الصناعية بالرياض.

بالتحديد، يثار الكثير من التساؤلات حول ماهية وطبيعة ومكافحة الغش التجاري في المجتمع الإلكتروني، من أهمها ما يلي:

- ١- هل تعتبر كافة الأشكال الجديدة للجريمة الإلكترونية غشا تجاريا؟ ومتى تعتبر غشا تجاريا ومتى لا تعتبر غشا تجاريا؟
- ٢- وإذا كان بعضا من تلك الجرائم الإلكترونية يعتبر غشا تجاريا، فهل تعتبر الجريمة في حد ذاتها غشا؟ أم ما يترتب عليه هو الغش؟
- ٣- هل يقتصر مفهوم الغش على الاحتيال الذي يلحق خسارة ملموسة بالمستهلك أو المؤسسة مباشرة فقط؟ أم أنه يمتد إلى كافة الصور الاحتمالية الأخرى، حتى أن لم توجد الخسارة الملموسة مثل سرقة وسائل التعريف، وغيرها؟ ومن ثم، فما هو التعريف الدقيق للغش التجاري الإلكتروني؟

٤- ما هي الأشكال الشائعة والخاصة للغش التجاري الإلكتروني؟ من هنا، فإنه من الأهمية بمكان الوقوف للتعرف على حدود انتشار حالات الغش المرتبط بالتجارة والاقتصاد على الإنترنت. ثم السعي لتحديد التعريف الدقيق للغش التجاري في المجتمع الإلكتروني، وماهية الصور والأشكال الشائعة والخاصة منه.

#### حدود انتشار الغش المرتبط بالتجارة والاقتصاد على الإنترنت: (١)

لقد شاع خلال عام ٢٠٠٤ انتشار العديد من جرائم الاحتيال الإلكتروني، حيث انتشر في هذا العام الكثير من الفيروسات المختلفة والبرامج المفجرة، كما زادت الرسائل الإلكترونية المزعجة بنسبة ٤٠%. أيضا شاع مصطلح الهاكرز مقترنا بالجريمة الإلكترونية الجديدة الذي أثار خوف ورعب الكثيرين من مستخدمي الإنترنت من الأفراد، أو المؤسسات، أو الجماعات،

(١) المرجع السابق.

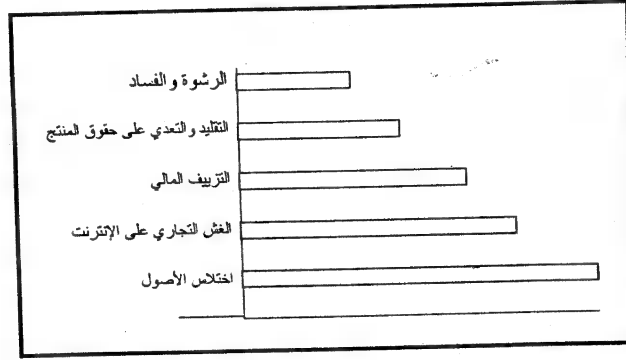
أو الحكومات والمنظمات والدول، بحيث أصبح مؤخراً يشكل أمراً خطيراً. وعلى الرغم من أن تلك الجرائم تعد بمثابة احتيالا إلكترونيا بحت، إلا أنها تستهدف جني الأموال، أو إلحاق الخسائر بأطراف أخرى، أو ضرب قدراتها التنافسية، كما أن بعضها قد يستهدف التشهير، أو الحصول على إثارة غير مشروعة، وغيرها من دوافع الإجرام المعروفة، والتي يوفر لها الفضاء الافتراضي مجالا خصبا، في ظل ما يكتسبه مرتكب تلك الجرائم من شروط حماية أوفر، وقدرة على التخفي، وانخفاض في حجم المخاطر، وقلة الرقابة أو البطء في استتعال الجريمة.

لقد نال موضوع الاحتيال التجاري على الإنترنت أهمية كبيرة خلال الآونة الأخيرة نظراً لانتشار استخدامات الإنترنت في كافة مجالات الحياة، بحيث أن جرائم الإنترنت احتلت نسبة هامة من بين الجرائم الاقتصادية الحادثة على مستوى كثير من الدول. فعلى سبيل المثال يوضح الشكل رقم (١) أن الغش التجاري على الإنترنت جاء في المرتبة الثانية من حيث أعلى نسبة في الجريمة الاقتصادية في هونج كونج، حيث شكلت نحو ٢٣% من إجمال الجرائم الاقتصادية الحادثة في الدولة، بل حتى أنها تفوقت على جرائم أخرى مثل التزيف والتقليد والرشوة<sup>(١)</sup>.

---

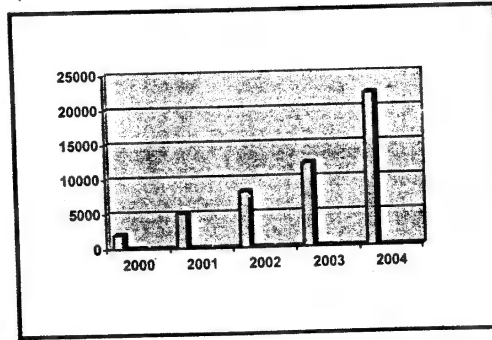
(١) المرجع السابق.

نصيب الغش التجاري على الإنترنت من إجمالي الجرائم الاقتصادية في هونغ كونج (%)



بالتحديد، لقد تزايدت حالات الاحتيال الحادثة على الإنترنت بشكل خطير، فحسب إحصائيات مركز شكاوي احتيال الإنترنت IFCC، يوضح الشكل رقم (٢) مدى الزيادة الكبيرة في إعداد الشكاوي من الأفراد والشركات اللذين تعرضوا للاحتيال والغش من جراء استخدام أو التجارة عن طريق الإنترنت.

تطور أعداد الشكاوي عن احتيال الإنترنت خلال الفترة (٢٠٠٠ - ٢٠٠٤)



ويتضح من الشكل رقم (٢) أنه خلال الفترة من يناير إلى ديسمبر من عام ٢٠٠٤ تلقى موقع المركز علي الإنترنت نحو ٢٠٧,٤٤٩ شكوى، وذلك بزيادة تبلغ نحو ٦٦,٦% عنها في عام ٢٠٠٣، حيث بلغت نحو ١٢٤,٥٠٩ شكوى، وذلك في مقابل نحو ١٩,٥٠٠ شكوى فقط في عام ٢٠٠٠، وهو الأمر الذي يشير إلى الزيادة الحادة والخطيرة في أعداد المستهلكين الذين تلحق بهم خسائر مادية نتيجة الاحتيال بالإنترنت.

أما من حيث حجم الخسائر المترتبة عن الأشكال الجديدة للاحتيال علي الإنترنت، فيوضح الجدول رقم (١) مدى التطور في حجم الخسائر نتيجة جرائم الكمبيوتر/ الإنترنت حسب نتائج المسح الذي أجراه معهد أمن المعلومات Computer Security Institute في عامي ٢٠٠٠، و٢٠٠٤<sup>(١)</sup>.

مقارنة بين حجم الخسائر الناجمة عن احتيال الإنترنت المرتبط بالتجارة خلال عامي ٢٠٠٠ و ٢٠٠٤ (دولار)

مصدر الخسائر/ الجريمة ونوع الهجوم	عام ٢٠٠٠	عام ٢٠٠٤
Theft of proprietary info. سرقة المعلومات المتعلقة بالملكية	٦٦,٧٠٨,٠٠٠	١١,٤٦٠,٠٠٠
Financial Fraud الاحتيال المالي	٥٥,٩٩٦,٠٠٠	٧,٦٧٠,٥٠٠
Telecom Fraud احتيال الاتصال	٤,٠٢٨,٠٠٠	٣,٩٩٧,٥٠٠

هذا وقد يكون من المهم التفرقة بين الغش/ الاحتيال الإلكتروني، وبين الغش/ الاحتيال المرتبط بالمجتمع الإلكتروني. فمصطلح الغش أو الاحتيال الإلكتروني يستخدم للدلالة علي كافة التصرفات التي يكون الكمبيوتر أو

(1) Computer Security Institute (Various Issues), CSI/ FBI Computer Crime and security Survey.

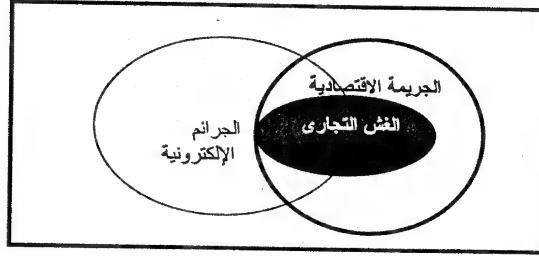
المصدر- دراسة أعنتها قطاع البحوث بالغرفة التجارية بالرياض.

الإنترنت أو المعلومات فيها هدفا للجريمة، كالدخول غير المصرح به واتلاف البيانات المخزنة في النظم، وغيرها. أما اصطلاح الغش أو الاحتيال المرتبط بالمجتمع الإلكتروني، فإنه يستخدم للتعبير عن تلك الجرائم التي يكون فيها الكمبيوتر أو الإنترنت أو المعلومات بمثابة وسائل أو أدوات لارتكاب الجريمة، كالاختيال المالي أو اختيال المزايدات أو التزوير، وغيرها. ويعرف الغش أو الاحتيال المرتبط بالمجتمع الإلكتروني في كثير من الأحيان بالجرائم الاقتصادية المرتبطة بالكمبيوتر Computer-Related Economic Crime، وهو تعبير يتعلق بالجرائم التي تستهدف معلومات قطاعات الأعمال أو تلك التي تستهدف البيانات الشخصية أو الحقوق المعنوية علي المصنفات الرقمية وكذلك جرائم المحتوى الضار أو غير المشروع، ولذلك لا يعبر عن كافة أنماط جرائم الكمبيوتر والإنترنت<sup>(١)</sup>. مما سبق يتضح أنه ليس كل الجرائم الإلكترونية تعتبر غشا تجاريا، بل وليس كل الجرائم الاقتصادية الإلكترونية تعتبر غشا تجاريا. فالغش التجاري يمثل أشكال وصورا معينة من الجريمة الاقتصادية المرتبطة بالكمبيوتر، والأخيرة في حد ذاتها تتخذ أشكال وصورا مختلفة من الجرائم الإلكترونية أو الجرائم المرتبطة بالكمبيوتر، وذلك كما يتضح من الشكل التالي:

---

(١) لمزيد من التفاصيل، يراجع: يونس عرب (٢٠٠١) العالم الإلكتروني: الوسائل والمحتوى والمزايا والسلبيات، مرجع سابق ذكره.





ولما كانت مجالات التجارة والمال والاقتصاد من أهم المجالات التي قد تنطوي علي أنشطة احتيالية في بيئة اليوم، فإنه من الأهمية بمكان التعرف علي ماهية وأشكال الاحتيال والغش المرتبطة بتلك المجالات في بيئة المجتمع الإلكتروني.

لذلك، تهدف كافة الأجزاء التالية من هذه الدراسة إلي تحديد والوقوف علي ماهية المفهوم الدقيق للغش المرتبط بالتجارة في المجتمع الإلكتروني، وتحديد أبرز الأشكال التي تم رصدها منه حتى الآن؟. ونظرا للجدل الكبير حول تحديد ماهية ومفهوم وحنود الغش في المجتمع الإلكتروني، فسوف تسعى هذه الورقة إلي تبني منهج يتجه أولا للوقوف علي الأشكال والصور الشائعة للغش التجاري في المجتمع الإلكتروني، ثم ستسعي إلي الوقوف علي مفهومه، وتحديد مدى الحاجة لتغيير المصطلح الذي يطلق عليه.

**الأشكال الخاصة والشائعة للغش المرتبط بالتجارة في المجتمع الإلكتروني:**

يسعي هذا البحث للوقوف علي أبرز الأشكال الشائعة للغش المرتبط بالتجارة في المجتمع الإلكتروني، وذلك من خلال مسح بعض أهم الدراسات التي تعرضت لتصنيف هذه الأشكال<sup>(١)</sup>.

(١) المصدر- دراسة أعدتها قطاع البحوث بالغرفة التجارية بالرياض.

لقد اتضح من تحليل أشكال الجريمة الإلكترونية أن الغش المرتبط بالتجارة في المجتمع الإلكتروني يمكن أن يحدث في العديد من الأشكال والطرق، وكما أنه قد يحدث للعديد من الأهداف. وعلى الرغم من تعدد هذه الأشكال، فسوف يركز الجزء التالي على الأصناف والأشكال الشائعة والخاصة المرتبطة بالتجارة والاقتصاد. وتتضمن تلك الأشكال بوجه عام الإنترنت كهدف أو كوسيلة لارتكاب جريمة الغش التجاري أو الاقتصادي.

**الغش في عمليات التجارة التي تتم بالاتصال المباشر على الخط:**

على الرغم من تحسينات السرعة والكفاءة التي تقدمها التقنيات المرتبطة بالإنترنت للتعاملات التجارية، إلا أنها تخلق أيضا مخاطر تجارية جديدة ومتعددة، فغالبا ما يتيح عنصر السرعة في إجراء الصفقات التجارية على الخط تسهيلات لحدوث الغش والاحتيال، نتيجة عدم وجود فترة انتظار Cooling-off بين أطراف الصفقات، يمكن أن تعكس شروط الاتفاقية المقترحة، ومن ثم الحصول على دليل مؤكد عن أهمية الموضوع أو تعريف كافي للطرف الآخر في الصفقة.

وأحيانا لا يكون بالإمكان تشغيل أو فرض عمليات الرقابة الداخلية الضرورية لمنع حدوث الغش الذي يحدث في التعاملات التجارية على الإنترنت، والتي يتم فيها بناء الاتفاقيات والدفع في آن واحد بشكل متزامن.

تتمثل هذه الدراسات فيما يلي:

- (1) Smith R. and G. Urbas (2001) "Controlling Fraud on the Internet: A CAPA Perspective", A Report For the Confederation of Asian and Pacific Accountants, Confederation of Asian and Pacific Accountants Australian Institute of Criminology, Research and Public Policy Series N. 39, Malaysia.
- Smith R. (2002), "Confronting Fraud in the Digital Age", op. Cit.
- Smith R and Grabosky (1996), "Fraud: An Overview of Current & Emerging Risks", & Trends & Issues in Crime and Criminal Justice, Australian Institute of Criminology, No. 62.

فضلا عن أن التعاملات الإلكترونية تتطوي علي قدر من الخسائر ينجم عن غياب المعلومات التي تتاح بسهولة في الصفقات التقليدية، والتي ترتبط بالخصائص الاجتماعية وسمات الأعمال الرئيسية سواء للبائع أو للمشتري والتي تستخدم لتوفير المصداقية والثقة في التعاملات التجارية. وتتمثل أبرز تلك الخصائص والسمات في المظهر وتعبيرات الوجه، ولغة الشخص، والصوت، والملبس، والتي جميعها لا يكون بالإمكان التعرف عليها حال إتمام الصفقة علي الإنترنت.

وترتكز المخاطر المرتبطة بسرقة المعلومات الشخصية من قواعد البيانات التي يمكن أن تستخدم بالتالي في ارتكاب الغش أو الاحتيال. فالمؤسسات التي تعتمد في صفقاتها علي التعاملات الإلكترونية تحتفظ بقواعد بيانات كبيرة للمعلومات الشخصية، متضمنة الأسماء والعنوانين، والحسابات البنكية، وتفاصيل البطاقات الائتمانية- مثلما تتضمن المعلومات الشخصية المرتبطة بنماذج الشراء التي يمكن أن تستخدم للأهداف التسويقية. ولما كانت بعض المعلومات لا يمكن الحفاظ علي سريتها، فتظهر فرص كبيرة لحدوث الغش، ليس فقط في إساءة استخدام وسائل التعريف، ولكن أيضا في القدرة علي الاحتيال علي ضحايا بشكل أكثر سهولة.

أيضا لما كانت التجارة الإلكترونية تتم بين أطراف تقع في دول مختلفة، فإنها تتضمن كافة المخاطر التقليدية المصاحبة لعمليات التجارة الدولية. بل أنه في حالة إتمام الصفقة علي الإنترنت تكون تلك المخاطر أكثر صعوبة في التعريف وتحديد موقع الطرف الآخر، ومن ثم أكثر صعوبة لنقل الرقابة القانونية لموقع أو دولة الطرف الآخر.

وترتبط معظم الاحتمالات في التعاملات التجارية التي تتم عبر الإنترنت بممارسات التضييق والخداع التي تعكس الأنشطة المشابهة التي تحدث باستخدام التقنيات الورقية التقليدية. ويتمتع المحتالون علي الإنترنت الآن بالقدرة علي الوصول المباشر للملايين من الضحايا في العالم وبأقل تكلفة ممكنة، علي سبيل

المثال مكائد المكافآت العالية، مثل مكائد الاحتيال الهرمي Pyramid scheme واحتيال Ponzi التي تستخدم سلسلة خطابات ورسائل إلكترونية، ومكائد فرص التجارة، ومزادات الاحتيال والجوائز والوئارية الخادعة.

وتتضمن الأشكال الأخرى للغش عبر استخدام الإنترنت عدم تسليم السلع والخدمات أو تسليم منتجات أو خدمات معيبة. وقد أصبحت تلك الأشكال أكثر انتشاراً في بيئة الأعمال التي تعتمد على منتجات وخدمات الكمبيوتر والخدمات المالية. فعلى سبيل المثال رغم الأهمية الكبيرة للتعاملات في الخدمات الصحية والطبية للمستهلك، إلا أنه قد تم اكتشاف العديد من حالات الغش والاحتيال المرتبطة بهما.

#### الاحتيال الهرمي: (١)

يعتبر الاحتيال الهرمي من أبرز أشكال الاحتيال التي برزت في البيئة العربية خلال السنوات القليلة الأخيرة. وهو عبارة عن برامج تسويقية واستثمارية احتيالية يتم بموجبها مكافأة المشاركين عند إقناعهم لأشخاص آخرين بالانضمام لهذه البرامج التسويقية. وبشكل أساسي، فإن هذا الهرم يتشكل عند قيام شخص واحد أو مجموعة من الأشخاص (شركة مثلاً) بجمع الأموال من مجموعة من الأشخاص (على شكل اشتراك لمرة واحدة مثلاً) والطلب من هؤلاء الأشخاص جمع الأموال من أصدقائهم بإقناعهم بالمشاركة في مثل هذا البرنامج وهكذا تبدأ الحلقة الأولى من الاحتيال. ويتم منح الوعود للمشاركين بحصولهم على عوائد مالية مجزية أو الترقية في الهيكل التنظيمي لمثل هذا المشروع التسويقي مقابل إقناعهم لأشخاص آخرين بالاشتراك. وتركز المشاريع التسويقية الهرمية على تبادل الأموال وتوظيف أشخاص جدد دائماً ولا يتعلق الأمر ببيع سلع أو منتجات إلا كغطاء لمثل هذه الأنشطة الاحتيالية، وخوفاً من السلطات الأمنية.

(١) المصدر - دراسة أعدها قطاع البحوث بالغرفة التجارية بالرياض.

### الغش في المزادات الإلكترونية:

يرتكز سوق المزاد عبر الإنترنت على الصورة، وتوصيف البضاعة من خلال نص مقتضب في الغالب. ونظرا لصعوبة تفحصها عن قرب لا يبق أمام المشتري سوى الثقة بعرضها. وحسب تقرير الاتحاد الفيدرالي للتجارة ومراقبة الاحتيال بالإنترنت، فإن جرائم الاحتيال التي تحدث في المزادات على الإنترنت تعتبر من أكثر جرائم الإنترنت شيوعا وانتشارا.

### الغش في نقل الأموال إلكترونيا:

أيضا يمكن أن يستخدم الإنترنت في القيام بالعديد من أشكال السرقة للأموال المنقولة إلكترونيا. فأحيانا يتم الحصول على بعض الوسائل المرتبطة بحماية المعلومات مثل كلمات المرور وتفاصيل الحسابات والتي يمكن من خلالها المحتالون من الوصول إلى قواعد البيانات الخاصة بشركات الأعمال والمؤسسات المالية. وفي بعض الظروف، قد ينقل المحتالون الأموال إلكترونيا من خلال إرسال أوامر بالبريد الإلكتروني. وعندما يصبح استخدام التجارة الإلكترونية أكثر انتشارا، فمن المتوقع تزايد إساءة استخدام الإنترنت المرتبط بنقل الأموال إلكترونيا.

### الغش في الأسهم والاستثمار:

يستخدم الإنترنت حاليا بشكل أكثر تنظيما في كافة أنشطة الشركات التي تتسع من مجرد تقديم العروض والتجارة في الأسهم إلى اعتماد الجهات الرسمية على حفظ المستندات الرسمية إلكترونيا. وبالفعل بدأت تظهر حالات وأمثلة عديدة للغش والاحتيال التي ترتبط بسوق الأسهم، حيث يستخدم بعض المحتالين الإنترنت حاليا لنشر معلومات خاطئة لجذب المستثمرين، أو للتلاعب بالأسهم.

### الغش المرتبط بوسائل التعريف:

تتمثل أحد أبرز الاستراتيجيات المستخدمة بشكل متكرر في ارتكاب الغش في خلق مستندات خاطئة لتعريف أحد وسائل التعريف. فالتعريف المسروق يتم إنشاؤه بشكل احتيالي، وبالتالي فإنه من الممكن أن يستخدم في سرقة النقود أو بأي شكل آخر غير قانوني، ومن ثم تجنب المساءلة والاعتقال.

وتكنولوجيا الإنترنت تجعل إخفاء أحد وسائل التعريف عملية أكثر سهولة. فالبريد الإلكتروني ومواقع الإنترنت قد يتم التلاعب بها من خلال تضمينها تفاصيل خادعة أو تغيير مصدر الرسالة التي تبدو أنها آتية من مستخدم آخر. من هنا، فإنه لا يوجد وسيلة لمعرفة المسارات التجارية لأولئك الأفراد المحتالون على الإنترنت.

### الاحتيال في التحصيل: (١)

قد تتجه مؤسسات الأعمال إلى تنفيذ أنشطة المشتريات والتحصيل إلكترونياً. فقد انتشرت خلال الفترة الأخيرة توجهات الشركات لاتمام عملية التحصيل وتوثيقها إلكترونياً. الأمر الذي يؤدي إلى مستويات أعلى من المرونة والثقة والتعاون الذي ينشأ بين أطراف عملية التحصيل. وتتنبأ عملية التحصيل الإلكتروني بعض مخاطر الاحتيال، نتيجة عدم وجود الرقابة الداخلية عندما يتم تنفيذ أنظمة التحصيل الإلكتروني الجديدة.

### مخاطر الاستشارات من الخارج: Outsourcing Risks

توجد أيضاً فرص مختلفة للجريمة الاقتصادية يمكن أن تحدث في الاتصال أو الربط مع الخدمات الاستشارية من الخارج، يرتبط ذلك بالتحديد بتكنولوجيا المعلومات وإدارة البيانات. فالاعتماد على موفري خدمة التطبيق (ASPs) - Application Service Providers - الذين يوفر الحيز

(1) المرجع السابق.

المطلوب لتخزين المعلومات الرقمية ينتمون لجهات أخرى- يولد مخاطر أن تستخدم تلك المعلومات لتنفيذ أغراض احتيالية أو بيعها بدون ترخيص. إن الاعتماد علي الاستثمارات الخارجية في خدمات تكنولوجيا المعلومات يخلق بوجه عام أيضا مخاطر للاحتيال أو الفساد، حيث قد يسيء المتعاقدون الثقة التي يحصلون عليها في إدارة بيانات سرية وحساسة.

#### الاحتياز علي الحكومات: (١)

يمكن أن تستفيد الحكومات من تكنولوجيا المعلومات والاتصالات في تقديم وإدارة خدماتها إلكترونيا ، إلا أنها بمؤسساتها ووكالاتها الرسمية أيضا قد تكون عرضة للاحتياز. وتزايد فرص هذا الاحتياز علي سبيل المثال لموفري خدمة الرعاية الصحية لموظفي القطاع الحكومي نتيجة التلاعب في أنظمة تنفيذ المطالبات إلكترونيا. وترتبط مخاطر أشكال المطالبات الإلكترونية بالتزيف أو التلاعب إلكترونيا، أو حل شفرة التوقيع الرقمي.

أيضا موظفي القطاع الحكومي قد يستخدمون تكنولوجيا المعلومات التي تتاح لهم لأغراض تسهيل العمل الرسمي بشكل غير مناسب في تنفيذ أغراض غير مرخصة لهم. فعلي الرغم من الكثير من التحذيرات الصريحة حول الاستخدام غير المناسب من جانب الموظفين للإنترنت في موقع العمل، تظهر هناك باستمرار حالات لإساءة بعضا منهم للإنترنت.

#### احتياز المستهلك: (٢)

علي الرغم من اتخاذ العديد من الاحتياطات لحماية المستهلك من التصرفات الاحتيالية علي شبكة الإنترنت، إلا أنه لا يزال هناك تزايد مستمر في أعداد الشكاوي التي تصدر من المستهلكين الذين يتعرضون لأفعال

---

(1) المرجع السابق.

(2) المرجع السابق.

احتمالية علي الإنترنت. وتزداد خطورة هذا الأمر بمعرفة مدى التنوع الكبير في أشكال وصور هذا الاحتيال التي تتغير بشكل طردي مع التقدم في تكنولوجيا المعلومات والاتصالات.

هذا ويمكن رصد أهم وأبرز الأشكال والصور الجديدة للاحتيال علي المستهلكين الأفراد علي الإنترنت، من خلال استعراض ومقارنة نتائج التقرير السنوي لمركز شكاوي الاحتيال علي الإنترنت الذي يديره United States Department of justice and Federal Bureau of Investigation ويوضح الجدول التالي أعلي عشرة أشكال للاحتيال علي الإنترنت في عامي ٢٠٠٠ و ٢٠٠٤:

#### الجدول

أعلي عشرة أشكال للاحتيال علي الإنترنت في عامي ٢٠٠٠ و ٢٠٠٤

٢٠٠٠ حسب نتائج تقرير Internet ٢٠٠٣ حسب تقرير Internet Fraud Complaint Center		٢٠٠٠ حسب نتائج تقرير Internet ٢٠٠٣ حسب تقرير Internet Fraud Complaint Center	
الشكل	%	الشكل	%
احتيال المزادات	٧٨	احتيال المزادات	٧١,٢
عدم التسليم المادي للمبيعات	١٠	عدم التسليم المادي للمبيعات	١٥,٨
سرقة خدمات الوصول علي الإنترنت	٣	احتيال بطاقات الائتمان	٥,٤
الاحتيال في العمل من المنزل	٣	احتيال الشيكات	١,٣
الاحتيال في قروض الدفعة المقدمة	٢	احتيال الاستثمار والأسهم	٠,٦
سرقة أجهزة وبرامج الكمبيوتر	١	احتيال المصادقية	٠,٤
احتيال الخطاب التيجيري	١	سرقة وسائل التعريف	٠,٣
احتيال بطاقات الائتمان	٠,٥	سرقة أجهزة وبرامج الكمبيوتر	٠,٢



يتضح من الجدول مدى الزيادة في نسب الغش والاحتيايل التي تلحق بالمستهلكين علي الإنترنت. كما يوضح الجدول مدى ارتفاع حالات الاحتيايل المرتبط بالتجارة والمال، فخلال عام ٢٠٠٤ ظهرت أشكال جديدة للاحتيايل التجاري لم تكن موجودة عام ٢٠٠٠، مثل احتيايل الشيكات واحتيايل الاستثمار والأسهم، والاحتيايل علي المؤسسات المالية. بل كان ملاحظا مدى الزيادة الحادثة في نسب الشكاوي المرتبطة باحتيايل بطاقات الائتمان، التي سجلت ارتفاعا من نحو ٠,٥% في عام ٢٠٠٠ إلي نحو ٥,٤% في عام ٢٠٠٤. الأمر الذي يستتج منه مدى الزيادة في حجم الخسائر التي لحقت بالمستهلكين علي مدى الفترة من عام ٢٠٠٠ إلي عام ٢٠٠٤، حيث ارتفعت هذه الخسائر من نحو ٣,٣٨٥ مليون دولار في عام ٢٠٠٠ إلي نحو ٦٨,١٤٠ مليون دولار في عام ٢٠٠٤<sup>(١)</sup>.

وجدير بالملاحظة أن أرقام الخسارة المرصودة عالية لا تعبر سوى عن الحالات التي تم رصدها في عدد قليل من الولايات الأمريكية، ولا تعبر بأي حال من الأحوال عن الوضع العالمي. الأمر الذي يمكن معه تصور مدى وحجم هذه الخسائر إذا تم رصدها علي مدى الولايات المتحدة ككل، بل مدى ضخامتها إذا أمكن رصدها عالميا.

#### الجدل حول مفهوم وحنود الغش التجاري في سياق المجتمع الإلكتروني:

من التحليل السابق لأشكال الاحتيايل علي الإنترنت، يتضح أن الغش أو الاحتيايل المرتبط بالتجارة أو الاقتصاد يحتل نسبة هامة من بين كافة أشكال الاحتيايل علي الإنترنت. بل أن الأشكال المرصودة للاحتيايل علي الإنترنت قد

(١) المرجع السابق.

كانت في غالبيتها ترتبط بالتجارة أو الاقتصاد. من هنا، يتضح أن الغش التجاري يمثل النسبة الأكبر داخل الأشكال المختلفة للاحتيال علي الإنترنت. إلا أنه لا تزال هناك كثير من الدراسات التي تثير الجدل والنقاش حول العديد من التساؤلات عن الأشكال الفعلية للاحتيال علي الإنترنت التي تعتبر غشا تجاريا. ويمكن تحديد أهم تلك التساؤلات فيما يلي:

- هل ينسحب مفهوم الغش التجاري إلي كافة الأشكال الاحتيالية المذكورة أعلاه أم أنه ينصب فقط علي صور الاحتيال التي تلحق بالمستهلك، والتي وردت في الفقرة (٩/٣/٨) فقط؟
- هل مفهوم الغش التجاري في بيئتنا العربية يأخذ فقط بتلك الأشكال والصور التي تلحق الخسائر بالأفراد المستهلكين أم ينسحب أيضا إلي تلك الأشكال والصور التي تلحق الأضرار بالمؤسسات والحكومة؟
- هل مصطلح الغش التجاري المستخدم حاليا يعتبر كافيا ومناسبا للتعبير عن كافة أشكال الغش والاحتيال في بيئة المجتمع الإلكتروني اليوم؟

#### **ماهية ومفهوم الغش في المجتمع الإلكتروني:**

لا يزال حتى الآن لا يوجد تعريف محدد لمفهوم الغش أو الاحتيال، حيث تعرفه دراسة (Graycar, and Russell, 2002) <sup>(١)</sup> بأنه يتضمن استخدام الكذب أو الخداع أو التضليل للحصول علي ميزة أو مصلحة غير مستحقة، وكانت من حق طرف آخر. وتشير الدراسة إلي أن الغش مثله مثل كافة الجرائم الأخرى يتضمن ثلاثة عناصر رئيسية، هي الدافع من حيث وجود العامل المحرك للإرادة والذي يوجه السلوك الاحتيالي كالانتقام والبغضاء

---

(1) Graycar, A. and S. Russell (2002), "Identifying and Responding to Electronic Fraud Risks", 30<sup>th</sup> Australasian Registrars' Conference, Australian of Criminology, Canberra, November.

وغيرها، ووجود الهدف أو الضحية للسلوك الاحتيالي، وغياب القدرة علي توفير الحماية.

أما دراسة (Auditing and Assurance Standards Board, 2002) <sup>(1)</sup> فتعرف الغش أو الاحتيال علي أنه يتمثل في أي تصرف أو سلوك متعمد يحدث من فرد أو العديد من الأفراد يرهق أو يتسبب في أعباء إضافية أية أطراف أخرى نتيجة استخدام ممارسات غير أخلاقية للحصول علي ميزة غير عادلة أو غير قانونية.

وعلي الرغم من تطبيق كلا من القوانين الجنائية ووسائل المكافحة المدنية لمكافحة ومنع حدوث الاحتيال، فإن دراية (Lanham, et al., 1987) <sup>(2)</sup> قد توصلت إلي أن جريمة الاحتيال تعتبر أحد الأمراض مستمرة الحدوث عبر الزمن. فبينما يوجد هناك انخفاض كبير في العديد من صور الجريمة مثل جرائم القتل والاعتصاب وجرائم الإيذاء الأخرى، لا يزال الاحتيال علي المستوى الفردي يسبب الألم والإيذاء للكثير من الأفراد. أما علي مستوى المجتمع، فإن حجم الخسارة فادحة، وتتضمن الكثير من ملايين الدولارات. بالتحديد، من الملاحظ تعدد تعريفات الغش في عصر المجتمع الإلكتروني، فأحيانا يعرف بالغش أو الاحتيال المعلوماتي أو غش الحاسب، وفي أحيان أخرى بالاحتيال بالإنترنت أو غيرها، إلا أنها تجتمع معا مع تركيزها علي أن الظاهرة الإجرامية المستحدثة تتمحور رغم اختلاف أنماط السلوك الإجرامي حول فعل الغش أو النصب أو الاحتيال في عمليات التجارة.

(1) Auditing and Assurance Standards Board, 2002, Australasian Auditing Standard AUS 210: the Auditor's Responsibility to Consider Fraud and Error in an Error in an Audit of a Financial Report, Auditing and Assurance Standards Board, Sydney.

(2) Lanham, D., and et. Al. (1987), Griminal Fraud, Law Book Company, Sydney.

وتعرف منظمة التعاون الاقتصادي والتنمية الغش والاحتيال الإلكتروني بأنه هو كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها<sup>(١)</sup>.

وتشير دراسة ( Government Printer for the state of Victoria, 2002)<sup>(٢)</sup> إلى أن الممارسة غير الأخلاقية توجد في قلب كافة أشكال الاحتيال، حيث يستطيع الفرد المخادع أن يحصل علي ميزة أو مصلحة مالية باستخدام تقنيات أو بنية تحتية تدعم التجارة الإلكترونية. كما تشير الدراسة إلى أنه لا يوجد قانون أو تشريع بسيط حتى الآن يتمكن من تعريف جريمة الاحتيال المرتبطة بإساءة الاستخدام في التجارة الإلكترونية الذي يستهدف الكسب المادي. فإساءة الاتصال أو التفاعل في البيئة الإلكترونية قد يعامل في طبيعته كجريمة سرقة أو كجريمة خداع، وتعد الممارسات غير الأخلاقية علي أنها جريمة ترتبط بتشريعات المستهلكين والممارسات التجارية حسب قوانين العديد من الدول.

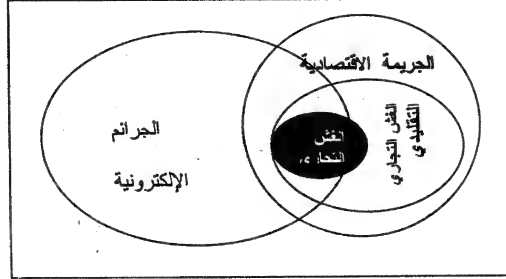
ولما كان تركيز هذه الدراسة علي الاحتيال في بيئة المجتمع الإلكتروني، فإنه من الواجب الاقتصار علي تلك الأفعال غير الأخلاقية التي تحدث بدافع الكسب المادي في هذه البيئة. بالتحديد، فإنه في بيئة الاتصال المباشر علي الإنترنت يوجد هناك فرص لا نهائية للغش الإلكتروني Electronic Fraud في شكل احتيالي.

(1) OECD (2003), OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders.

(2) Government Printer for the state of Victoria, 2002, Inquiry into Fraud and Electronic Commerce: Emerging Trends and Best Practice", Discussion Paper, Drugs and Crime Prevention Committee, DCPS, Parliament of Victoria, October.

وقد توصلت دراسة ( Victoria, 2002 ) إلي صياغة تعريف واسع لمفهوم الاحتيال التجاري الإلكتروني يتضمن كافة المشكلات والقضايا مثل تدمير البرامج والأنظمة من خلال التخريب المتعمد الذي يحدث عندما تصيب الفيروسات الكمبيوتر، أو الجرائم الأخرى التي تتضمن نشر المواد البغضية أو غير القانونية، علي سبيل المثال عندما تسعى الشركات أو الأفراد لبيع الصور الإباحية علي الإنترنت. مع ذلك، بعض الجرائم لا تشكل جزء من ذلك التعريف الواسع إذا لم تتضمن عنصر الخداع أو الممارسة غير الأخلاقية، والتي فيها يتم ارتكاب الجريمة بهدف الحصول علي كسب مادي.<sup>(١)</sup>

علاقة الغش التجاري الإلكتروني بالغش التجاري والجرائم الإلكترونية



وإذا كانت هذه الورقة قد توصلت إلي أن الغش المرتبط بالتجارة في المجتمع الإلكتروني يعتبر أحد أشكال الجرائم الإلكترونية، وفي نفس الوقت يعتبر<sup>(٢)</sup> أحد أشكال الجرائم الاقتصادية، فإن هذه الورقة تسعى للتقدم خطوة أخرى للأمام بتحديد موقع وعلاقة هذا الشكل من الغش التجاري الحادث في

(1) المصدر - دراسة أعدتها الغرفة التجارية بالرياض.  
(2) المصدر - قطاع البحوث بالغرفة التجارية الصناعية بالرياض.

سياق المجتمع الإلكتروني، وذلك كما يتضح من الشكل ، حيث يتضح منه أن هناك شكلا جديدا من الغش التجاري يقع بالكامل داخل نطاق الغش التجاري، وأيضا داخل نطاق الجريمة الإلكترونية، فضلا عنه أنه يقع داخل نطاق الجريمة الاقتصادية أيضا. ولكي يتم تمييز هذا الشكل من الغش عن الغش التجاري التقليدي، فتسعي هذه الورقة لتعريفه بالغش التجاري الإلكتروني.

وبناء عليه وفي ضوء التحليل في الأجزاء السابقة، يمكن الوقوف على تعريف محدد للغش والاحتيال التجاري الإلكتروني من خلال التركيز على الدوافع، وبشكل يتسق مع التطورات المعاصرة ويتكيف مع مدى السرعة الكبيرة في تطور حالات الغش في بيئة المجتمع الإلكتروني، فيعرف الغش التجاري في المجتمع الإلكتروني بأنه:

«هو كل فعل أو ممارسة غير أخلاقية تستخدم فيها تقنيات المجتمع الإلكتروني وتهدف إلى تحقيق كسب مادي غير مشروع»<sup>(1)</sup>.

وبناء على هذا التعريف فإنه يمكن تقرير ما يلي:

أولا- أنه لا فرق بين المستهلك الفردي أو المؤسسة أو الحكومة في تصنيف حالة الغش أو الاحتيال التجاري، ومن ثم فإن كافة الأشكال المرصودة للغش التي ترتكب في حق الحكومات أو المؤسسات تعتبر غشا تجاريا. ثانيا- أن تقرير إذا ما كان أحد أشكال الجريمة أو الاحتيال غشا تجاريا، يرتبط بشكل الجهة المتضررة بقدر ما يرتبط بأنه نجم عن نشاط مرتبط بالتجارة وألحق خسارة بهذه الجهة المتضررة.

ثالثا- أن كافة الأنشطة والمجالات التي تلحق خسائر بالأفراد أو المؤسسات سواء الحكومية أو الخاصة على الإنترنت تعتبر غشا تجاريا.

---

(1) المرجع السابق.

رابعاً- أن مصطلح غش المستهلك أو الغش التجاري للمستهلك بات مفهوماً ضيقاً لا يتناسب مع الغش التجاري في المجتمع الإلكتروني الذي قد يلحق بالمؤسسات والحكومات. لذلك فتقترح هذه الورقة إعادة تسميته بالغش التجاري الإلكتروني.

خامساً- أن الغش التجاري الإلكتروني يشكل نوعاً خاصاً من الغش التجاري الذي يرتبط بالمجتمع الإلكتروني، إلا أنه يتميز عن الغش التجاري التقليدي في أنه قد يرتكب بحق مؤسسات الأعمال أو الحكومات.

سادساً- أن البيئة العالمية تعج حالياً بالعديد من أشكال الجرائم الإلكترونية. وقد اتضح من تحليل أشكال الخدمات والمنافع الإلكترونية، وأيضاً تحليل أشكال الغش في المجتمع الإلكتروني أن هناك ارتباطاً كبيراً وبارزاً بين شكل الخدمة أو المنفعة الإلكترونية الجديدة وبين الغش الإلكتروني. ولما كانت هذه الخدمات والمنافع متجددة ومتطورة بشكل متسارع، فإن تحديد أشكال الغش التجاري المحتملة في المجتمع الإلكتروني يعد مهمة في غاية الصعوبة. وبالتالي فإن عملية مكافحته قد تكون بمثابة المستحيل على الأقل في المراحل الأولى لحدوثه.

سابعاً- أن هناك فجوة بين حالات الغش الحادثة وبين جهود المكافحة. ويمكن تفسير هذه الفجوة بنوعين من الصعوبات، هما صعوبة رصد حالاته وإثباته، وصعوبة اكتشاف وسد الثغرة التي نجم عنها.

ثامناً- يمكن تحديد الأسباب الرئيسية وراء صعوبة إثبات الغش التجاري الإلكتروني فيما يلي<sup>(١)</sup>.

تاسعاً- أنه كجريمة لا يترك أثراً بعد ارتكابه.

---

(١) محمد محمد شتا، (٢٠٠١)، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية.

عاشرا- صعوبة الاحتفاظ الفني بآثاره إن وجدت.  
حادي عشر- أنها تعتمد علي الخداع في ارتكابها والتضليل في التعرف علي مرتكبها.

الثاني عشر- أنه يعتمد علي قمة الذكاء في ارتكابه.

الثالث عشر- يترتب علي هذه الصعوبات مشكلات خطيرة، من أبرزها الاعتماد علي أسلوب سد الثغرات في مكافحة الأشكال الجديدة للجريمة والاحتيال الإلكتروني. وتكشف الإحصائيات عن حالات الجريمة الإلكترونية مدى خطورة الاعتماد علي أسلوب سد الثغرات في مكافحة الجريمة الإلكترونية، حيث تشير علي أن كل شكل جديد من أشكال الاحتيال الإلكتروني يبرز شكل محدود في البداية، ثم لا يلبث أن ينمو، حتى ينتشر بشكل كبير، ثم لا يلبث أن يضمحل ويزول في النهاية.

من هنا يتضح مدى خطورة الغش التجاري الإلكتروني الذي يتسبب كل شكل جديد حادث منه في كم هائل من الخسائر حتى يتم التوصل إلي الطريق أو الوسيلة الفعالة للتغلب عليه ومكافحته. الأمر الذي يوضح مدى القصور في الاعتماد علي أسلوب سد الثغرات في مكافحته، بما يعزز من الدعوى إلي إيجاد أسلوب بديل أكثر فعالية للوقاية من الغش التجاري قبل وقوعه. وهو ما يستلزم مزيد من الاهتمام بالتعرف علي التسهيلات التي يمكن أن تقدمها أي خدمة أو منتج إلكتروني جديد، بالشكل الذي يضمن عدم القدرة علي استغلاله في الغش أو الاحتيال في العمليات التجارية، وذلك بهدف تقليص حجم الخسائر الناجمة عن الغش قبل حدوثه.

الخلاصة: تعرضت هذه الدراسة لدراسة وتحليل ماهية وأشكال الغش التجاري في ظل التطورات المعاصرة، حيث تناول بالتحليل دراسة ثلاث نقاط رئيسية، هي ماهية التطورات المعاصرة في البيئة الاقتصادية العالمية،



وماهية وأشكال الجرائم الإلكترونية الناجمة عن تلك التطورات، والغش التجاري في المجتمع الإلكتروني الجديد.

وتناولت النظم في تكنولوجيا المعلومات والاتصالات وعولمة الأسواق كأحد أبرز التطورات التي حدثت خلال الآونة الأخيرة، وتوصلت إلى أن تلك التطورات علي الرغم مما أدت إليه من مزايا وأثار إيجابية، إلا أنها ساعدت بشكل رئيسي في نفس الوقت علي ظهور أشكال وصور جديدة من الجرائم، عرفت بالجرائم الإلكترونية.

ومن خلال استعراض أبرز أشكال وصور تلك الجرائم الجديدة، اتضح أن قدر كبير منها يرتبط بمجالات التجارة والمال والاقتصاد، أو ما يعرف بالجريمة الاقتصادية المرتبطة بالكمبيوتر أو الإنترنت. ثم انتقل التحليل للتركيز علي صور الجريمة المتمثلة في الغش والاحتيال المرتبط بالتجارة والمال والاقتصاد أو لتقنين ماهية الغش التجاري في المجتمع الإلكتروني الجديد.

وتوصل التحليل إلى أن الغش التجاري يمثل نسبة هامة من الجرائم الإلكترونية، بل ونسبة هامة من الجرائم الاقتصادية المرتبطة بالكمبيوتر. وفي سبيل تحديد والوقوف علي المفهوم الدقيق للغش التجاري في المجتمع الإلكتروني كان لابد للدراسة من التعرف علي أبرز الأشكال والصور التي يتخذها الغش التجاري في هذا المجتمع الجديد، حيث اتضح أن هناك أشكالاً شائعة وخاصة للغش المرتبط بالتجارة في المجتمع الإلكتروني، من أبرزها الغش في عمليات التجارة التي تتم بالاتصال المباشر علي الخط، والغش في المزايدات الإلكترونية، والغش في نقل الأموال إلكترونياً، والغش في الأسهم والاستثمار، والغش المرتبط بوسائل التعريف، والاحتيال في التحصيل، ومخاطر الاستشارات من الخارج، والاحتيال علي الحكومات، وسرقة الخدمات، وتزوير المعلومات، وسرقة مواصفات مواقع النت واحتيال المستهلك.

ثم سعت لإزالة الجدل القائم حول مفهوم وحدود الغش التجاري في المجتمع الإلكتروني، حيث عرفت الغش التجاري في المجتمع الإلكتروني يعرف بأنه "هو كل فعل أو ممارسة غير أخلاقية يمكن أن تتسبب أو تلحق خسارة مادية بالطرف الآخر المتعاقد معه".

ثم سعت لإزالة الجدل المرتبط هل الغش التجاري هو فقط ذلك الغش الذي يرتبط بالمستهلك الفردي، بأن توصلت إلي أن كافة الأفعال والتصرفات الاحتيالية التي ترتكب بحق المستهلكين الأفراد أو المؤسسات أو حتى الحكومات تعتبر من قبيل الغش التجاري.

كما توصلت الدراسة إلي ضيق مفهوم الغش التجاري الحالي، بحيث أنها اقترحت ضرورة تمييز الغش التجاري التقليدي الذي يحدث في بيئة العالم المادي في السلع والخدمات عن الغش في بيئة العالم الإلكتروني، بحيث أنها تقترح تسمية هذا الشكل الجديد من الغش بالغش التجاري الإلكتروني.

من هنا، فيمكن القول بأن أشكال الغش التجاري الإلكتروني الجديد تنطوي علي قدر كبير من الخطورة بالشكل الذي يستلزم مزيد من الاهتمام بالاعتراف علي التسهيلات التي يمكن أن تقدمها أي خدمة إلكترونية جديدة، وإمكانيات استغلالها في الاحتيال والغش قبل طرحها للجمهور، وذلك بهدف تقلي حجم الخسائر الناجمة عن الغش والاحتيال قبل حدوثه.

من هنا فإن هذه الدراسة تعتمد علي تبني الفكر الوقائي في الغش التجاري الإلكتروني، حيث أن الاعتماد علي الفكر الحمائي قد ثبت أنه غير فعال وغير كافي لمكافحة الغش التجاري الإلكتروني<sup>(١)</sup>.

---

(1) دراسة قد أعدتها الغرفة التجارية الصناعية بالرياض وتناولت حول الغش التجاري وهي مرتبطة بموضوع الكتاب وقد أوردتها لأهميتها لإيضاح فكرة الجريمة المعلوماتية.

**الفصل الرابع**  
**مكافحة الجرائم المعلوماتية**



## أمن المعلومات وحقوق الإنسان... رؤية حذر

لقد تدنت مؤشرات حقوق الإنسان العربية في مجالات عدة وتراءى لبعض إن ما يشهده العالم من تطور تكنولوجي بات من السهل لأى مستفيد عربي أن يهضم تلك المخرجات التقنية الحديثة دون الإصابة بعسر في الهضم... ولعله يخيّب ظني إذ أتوقع تدني مؤشر حقوق الإنسان من المعلومات، المعلومة التي أصيبت بانتكاسة اقتصادية شأنها شأن السلعة سواء في إنتاجها أو تسويقها أو جودتها، إلا أن الخطر الأكبر الذي يحيق بأمن المعلومات هو تفرغها من مضمونها وقيمتها والقدرة على حمايتها، ذلك أن الفرد العربي اعتاد على التلقين التقني دونما تفعيل أو مشاركة في تلقين مرتد ( feed back ) وتلك هي محك القضية وذاك هو الجذع الذي نترامي عليه كل أوراق الموضوع.

البيئة الرقمية، مجتمع المعلومات ومجتمع الأمية المعلوماتية، خريطة المعرفة في العالم العربي... مصطلحات جديدة لعالم آخر، تلك هي محاور الورقة التي قدمها الباحث<sup>(1)</sup> في دراسة مستفيضة قدمت في مؤتمر بجامعة القاهرة في أكتوبر ٢٠٠٤ وناقشت التصور الحذر لسلبيات منظومة المعرفة الجديدة على المستفيد العربي.

لقد أمسى الاتجاه المستمر والمتدفق نحو الاستخدام الآلي في إنجاز الأنشطة المختلفة للإنسان يبشر بمجتمع يعيش بلا ورق مطبوع أو مخطوط أو بعبارة أخرى يمهّد لقيام مفهوم جديد للمجتمعات<sup>(2)</sup>، وهو المجتمع اللورقي ( paperless )، أو المجتمع الرقمي ( Digitations Society ).

(1) <http://www.annabaa.org/nbahome/nba74/amn.htm>

/ محمد محمود مكاوي باحث بدار الكتب والوثائق القومية - مصر.

(2) المرجع السابق.

## مجتمع المعلومات (٢): (Information Society):

ويقصد بمجتمع المعلومات أيضاً جميع الأنشطة والموارد والتدابير والممارسات المرتبطة بالمعلومات إنتاجاً ونشراً وتنظيماً واستثماراً. ويشمل إنتاج المعلومات أنشطة البحث على اختلاف مناهجها وتنوع مجالاتها، بالإضافة إلى الجهود والتطوير والابتكار على اختلاف مستوياتها كما يشمل أيضاً الجهود الإبداعية، والتأليف الموجه لخدمة الأهداف التعليمية والتثقيفية والتطبيقية.

## مجتمع الأمية (Illiteracy):

يعتبر مصطلح الأمية من المصطلحات الرجة الفضفاضة، فليست الأمية هي فقط عدم القدرة القرائية أو الكتابية بل هناك العديد من القراءات التي توضح هذا المفهوم. ففي ظل هذه الطفرة المعلوماتية التي تحيط بالكيان المعرفي، قد نشأت الأمية الحاسوبية (Computer Illiteracy) التي توضح عدة قدرة بعض المتعلمين على التعامل مع الحاسب الآلي، كما أن هناك الأمية المعلوماتية (Information Illiteracy) التي تشير بشكل أو بآخر إلى عدم قدرة المتعلمين أو حتى مستخدمي الحاسب الآلي عن الوصول إلى معلوماتهم أو حتى التعامل مع مصادر المعلومات في ظل العمل المعلوماتي (information Work) المعقد، وهذان المفهومان متناوبان بالتداخل.

## البيئة الرقمية وأمن المعلومات:

مما لا شك فيه أن التقنية الرقمية الحديثة قد أثرت بشكل جدي على هوية وقيمة المعلومات، وبات من السهل اقتناء واختزال بل واختراق الأنساق المعلوماتية المختلفة، وأصبح من الممكن تكسير الحواجز الأمنية التي تحمي المعلومة، خصوصاً بشكلها الرقمي الجديد، وهذه النظرة لا تمثل التفكير برؤية تشاؤمية بل هي رؤية حذر وتأن محاولة لفهم واقع الهوية العربية.

### أمن المعلومات (٣) (Information Security):<sup>(١)</sup>

أمن المعلومات هو قضية تبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنية، هو الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهذا هو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها ( جرائم الكمبيوتر والانترنت).

إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات - سواء الناحية التقنية أو الادائية - وكذا هدف التدابير التشريعية في هذا الحقل، ضمان توفر العناصر التالية لأي معلومات يراد توفير الحماية الكافية لها:

١- السرية أو الموثوقية **ONFIDENTIALITY** : وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

٢- التكاملية وسلامة المحتوى **INTEGRITY** : التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص، لن يتم تدمير المحتوى أو تغييره أو العبث به في أى مرحلة من مراحل المعالجة أو للتبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

٣- استمرارية توفر المعلومات أو الخدمة **AVAILABILITY** : التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع

---

(1) <http://www.annabaa.org/nbahome/nba74/amn.htm>.

المعلومات وتقديم الخدمة لمواقع المعلوماتية وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

٤- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به -Non repudiation : ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو واقعها، إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين.

دول الخليج العربي وخريطة تأمين المعلومات<sup>(١)</sup>:

لقد حذر خبرا دوليون في أغسطس ٢٠٠٤ من تفاقم أزمة أمن المعلومات لدول المنطقة وكانت الاحصاءات تشير إلى أن الاحتياطي المخصص لدول المنطقة العربية للإنفاق على أمن المعلومات حتى عام ٢٠٠٤ لا يتجاوز ٢٠٠ مليون دولار في حين أن المطلوب توفيره هو ٥ مليارات دولار، وأشارت التقديرات إلى أنه يتعين على القطاع الخاص بمعاونة القطاع الحكومي التعاون في مجال المصارف بشكل خاص وضرورة أن تتبنى استراتيجية مؤثرة لأمن المعلومات.. وانتقد التقرير تساهل المؤسسات والمصارف في الحفاظ على سرية وأمن المعلومات وأرجع التقرير، القصور إلى عدم وجود هيئة أو مؤسسة تقوم بتنظيم أمن المعلومات كما أشار التقرير الذي اعتمدته مؤسسة ( AGT ) الألمانية إلى خطورة هذا الوضع على الأمن القومي للدول العربية التي تمتلك أكثر من ٥٠ ألف مؤسسة متخصصة، ورغم ذلك تعاني من مشاكل في نشاطها في ظل لفتصاد الأمن، وأشار التقرير إلى أنه سيعقد مؤتمرا بمبادرة ألمانية ومشاركة عربية في برلين تحت عنوان ( كيفية الأمن للاقتصادات العربية ضد المخاطر الإلكترونية).

---

(١) الموقع السابق.



أولاً: الإمارات العربية وفي هذا الإطار نشير إلى أن الإمارات العربية المتحدة أعلنت عن افتتاح مركز لدراسة أمن الشبكات والمعلومات في الشرق الأوسط وقد وقع الشيخ نهيان بن مبارك وزير التعليم العالي والبحث العلمي على إنشاء مركز التميز بكلية تقنية المعلومات بجامعة الإمارات محققاً بذلك سبقاً تقنياً في مجال البيئة الرقمية في منطقة الحزام العربي وقد خصص لهذا السبق التقني نخبة من المتخصصين في أمن الشبكات وتقنية المعلومات وخبراء متخصصون في أمن المعلومات في المؤسسات الحكومية.

ثانياً: المملكة العربية السعودية لقد أشارت ضوابط استخدام<sup>(١)</sup> الإنترنت في المملكة التي أعدت من قبل لجنة الإنترنت الأمنية الدائمة، التي ترأسها وزارة الداخلية أن يلتزم كل مستخدم الإنترنت بالمملكة العربية السعودية بالامتناع عن نشر أو الوصول إلى المعلومات التي تحتوي على بعض مما يأتي:

- ١- كل ما يخالف أصلاً وشرعاً الإسلام وشريعته وما يتضمن القذف أو التشهير بالأفراد وكذلك كل ما من شأنه تحريض الإجرام أو الدعوة إليه.
- ٢- التقارير والأخبار التي لها مساس بسلامة القوات المسلحة السعودية.
- ٣- نشر الأنظمة أو الاتفاقيات أو المعاهدات أو البيانات الرسمية للدولة.
- ٤- الدعوة إلى المبادئ الهدامة أو زعزعة الطمأنينة العامة أو بث التفرقة بين المواطنين.

وأمثالاً لتأمين المعلومات التجارية فقد نصت بعض التعليمات التجارية على التزام جميع الشركات والأفراد المستفيدين من الخدمة بما يأتي:

- ٥- عدم مزاوله أي نشاط عمل عبر الشبكة كالبيع أو الإعلان أو التوظيف أو غير ذلك إلا بموجب التراخيص أو السجلات التجارية سارية المفعول.

---

(١) الموقع السابق.

٦- عدم مزاوله أنشطة الاستثمارات المالية أو طرح أسهم للاكتتاب إلا لحاملي التراخيص اللازمة لذلك.

٧- عدم الترويج أو البيع للأكوية أو السلع الغذائية التي تحمل ادعاءات طبية أو لمواد التجميل إلا لما هو مسجل ومصرح به من قبل وزارة الصحة. ثالثاً: الكويت وبالنسبة للكويت فقد أدرجت تحت المراقبة الخاصة للملكية الفكرية ومن أجل الخروج من هذه الدائرة قدم حلف الملكية الفكرية الدولي عدة شروط أهمها<sup>(١)</sup>:

١- الإعلان من أعلى مستوى في الحكومة الكويتية بعدم السماح للقرصنة.

٢- القيام بحملات متواصلة ومنظمة ضد القرصنة.

٣- الإعلان عن الحملات للحصول على تأثير رادع.

٤- فرض غرامات إدارية ومالية ومحاكمة المخالفين.

٥- تعديل قانون حماية حقوق الناشر لينسجم مع اتفاقية الجوانب التجارية لحقوق الملكية الفكرية.

وفى هذا الإطار يرصد تقرير تحالف البرمجيات ( BSA ) ( نفس المصدر) أكثر الدول انتهاكا لحقوق الإنسان الفكرية في العالم وهم ٢٤ دولة جاءت قطر في المؤتمر ٧ والبحرين في المؤشر ١١ وعمان ١٢ والكويت ١٤ وينكر التقرير أن الصناعة المعتمدة على حقوق النشر بالكويت تخطت ٢٥ مليون دولار نتيجة نسخ البرمجيات وهي نسبة متواضعة من إجمالي خسائر القرصنة التي بلغت ١٠ مليارات دولار عام ١٩٩٩ والشئ المخيف أن تظل الكويت واحدا من أعلى معدلات القرصنة في العالم وفي الخليج.

---

(١) لموقع سبق.

وإذا كانت مصادر المعلومات الورقية ستظل تتعايش مع مصادر المعلومات الإلكترونية إلا أن الأخيرة ستكون هي المتفوقة والمهيمنة في المستقبل فسيظل الزحف الإلكتروني المتنامي والشبكات المتطورة وذلك للأسباب الآتية:

١- توفر للباحث كمّاً ضخماً من البيانات والمعلومات سواء من خلال الأقراص المتراصة، أو من خلال اتصالها بمجموعات المكتبات ومراكز المعلومات والمواقع الأخرى.

٢- تكون السيطرة على أوعية المعلومات الإلكترونية سهلة وأكثر دقة وفعالية من حيث تنظيم البيانات والمعلومات وتخزينها وحفظها وتحديثها مما سينعكس على استرجاع الباحث لهذه البيانات والمعلومات.

٣- يستفيد الباحث من إمكانات المكتبة الإلكترونية عند استخدامه لبرمجيات معالجة النصوص، ولبرمجيات الترجمة الآلية عند توافرها، والبرامج الإحصائية، فضلاً عن الاستفادة من إمكانات نظام النص المترابط، والوسائط المتعددة (multimedia).

٤- تخطي الحواجز المكانية والحدود بين الدول والأقاليم واختصار الجهد والوقت في الحصول على المعلومات عن بعد، وبإمكان الباحث أن يحصل على كل ذلك وهو في مسكنه أو مكتبه الخاص.

٥- التمكن من <sup>(١)</sup> استخدام البريد الإلكتروني والاتصال بالزملاء في المهنة والباحثين الآخرين، وتبادل الرسائل والأفكار مع مجموعات الحوار ( Discussion groups ) وتوزيع الاستبيانات واسترجاعها.

٦- تنتج هذه المكتبات للباحث فرصة كبيرة لنشر نتائج بحثه فور الانتهاء منها في زمن ضاقت فيه المساحات المخصصة للبحوث على أوراق

---

(1) لموقع سابق.

الدوريات. هناك العديد من المبررات التي دعت إلى التحول إلى المجتمع الرقمي منها ما هو اقتصادي ومنها ما هو مهني ومنها ما هو جغرافي وزمني أهمها الآتي:

١- زيادة الإنفاق على الأوعية التقليدية واستغلال الوقت والجهد في عمليات البحث.

٢- حرص المكتبات على البقاء في ظل سوق خدمات المعلومات.

٣- زيادة كثافة الأوعية التقليدية.

٤- قدرة النظام الرقمي على مد الخدمة وكسر الحواجز الجغرافية.

خصوصية مجتمع المعلومات الرقمي والانعكاسات على حقوق الفرد من المعلومات.

#### البيئة الرقمية العربية... مؤشرات ودلالات: (١)

لقد أشارت تقارير الأمم المتحدة إلى إتساع الفجوة المعلوماتية بين البلدان العربية والبلدان المتقدمة، وأوضح أن هناك نسبة ١,٢% من المواطنين العرب يمتلكون حاسباً، ونصف هذا العدد يستخدم خدمة الإنترنت، وأشار التقرير إلى أن معظم الدول العربية عدا الإمارات والكويت تتساوى جميعها في درجة افتقارها لتقنية المعلومات والاتصالات.

كما أظهرت المسوحات العالمية لمحتوى الإنترنت أن اللغة العربية لا تتجاوز ١% من كل المحتوى في حين تمثل اللغة الإنجليزية ٦٨,٨% من الإجمالي وهذه النسبة الضئيلة للوطن العربي وللأمة الإسلامية تكاد تكون مستقرة رغم كل محاولات إنقاذها.

هذا ولم تستخدم التقنية المعلوماتية حتى الآن شكلاً كافياً في الوطن العربي، ولم يتم تقدير دور المعلومات في عملية التنمية قدرها الصحيح. وما

---

(١) لمزيد من السابق.

رالت هناك عوامل متعددة تؤثر تأثيراً مباشراً في أنشطة المعلومات ومن هذه العوامل:

١- الفجوة الاقتصادية بين الدول العربية، فهناك دول غنية تستطيع اقتناء أحدث نظم تقنية المعلومات وهناك دول فقيرة تنتظر إلى تقنية المعلومات كرفاهية علمية غير مطلوبة قبل توفير الغذاء والسكن لشعبها.

٢- الاختلاف الشديد في الكثافة السكانية للدول العربية، فهناك دول مكتظة بالسكان، وتستطيع أن تصدر فائضاً من القوى العاملة المدربة والمؤهلة في مجال تقنية المعلومات، في حين أن هناك دولاً محدودة السكان لا تتوفر لديها الأطر الفنية القادرة على تغطية وشمول هذا المجال، قبل مجالات العلوم والتقنية الأكثر إلحاحاً وأهمية بالنسبة للدولة.

٣- الاختلاف الكبير في مستويات العلوم والتقنية والمعرفة بشكل عام بين الدول العربية، فهناك مراحل متقدمة في هذه المجالات في حين أن هناك دولاً ما زالت في أول الطريق.

٤- النمو المتزايد في عمليات الاستثمار والأنشطة والأعمال التجارية، التي تدعو بالتالي إلى ضرورة توفر نظم المعلومات الحديثة والتقنية الإعلامية لتواكب الحركة العالمية، خاصة بعد ارتباط هذه الأنشطة بالأسواق العالمية التي استخدمت تقنية المعلومات منذ فترات طويلة وأصبح لها دراية وخبرة بهذه المجالات وببأثيراتها على تنمية الاستثمارات والأنشطة التجارية.

٥- اختلاف المفاهيم والمعاني المتصلة بالتقنية المعلوماتية، حيث ما زالت هذه المفاهيم غير موحدة بين الدول العربية، ولكل منها معني مغاير من دولة إلى أخرى، بل أحياناً من هيئة إلى أخرى داخل الدولة الواحدة.

٦- ضعف دور المنظمات العربية المتخصصة في مجال تقنية المعلومات، بل أن بعضها لم يتواجد بعد على الساحة العربية، مثل خلق

مؤسسة عربية لإعداد حواسيب عربية تستخدم ( شيفرة ) عربية ولغات برمجة عربية وإعداد حزم برامج وقواعد بيانات عربية...الخ<sup>(١)</sup>.

٧- ضعف دور مراكز المعلومات الوطنية المتوفرة بالدول العربية، فغالباً لا تتوفر خطط وطنية لهذه المراكز، وإذا توفرت قد تحيد عنها أو تتوقف عن تنفيذها لأسباب داخلية أو لأسباب خارجة عن إرادتها ( مثل تقليص ميزانيتها أو نقل تبعيتها الإدارية...الخ).

#### باحثو المعلومات في المكتبة الإلكترونية:

لقد أصبح هناك مؤثران يوضحان دور الأخصائي ( باحث المكتبات)، المؤشر الأول يشير إلى تضائل أو محدودية دور الأمين في ظل تأثير التقنيات الحديثة المترامية، ويشير المؤشر الثاني إلى تأييد دور باحثي المكتبات والمعلومات واستمرارية الدور المنوط به.

**المؤشر الأول:** الخاص بتضائل دور المكتبي يستند إلى التقنيات الحديثة باعتبارها أضافت متغيراً جديداً وبعداً آخر للبنية أو التوسط المعلوماتي ( Information meditating )، فالمعلومات على الخط المباشر وعلى الشبكة العنكبوتية ( www ) أصبحت داخل وخارج المكتبة وبإستطاعة المتصفح على الحاسب أن يكسر حاجز الوصول إلى المعلومات عن طريق التنفيذ أو الوصول إلى شبكات المعلومات البعيدة بل والقدرة على تفريغ هذه المعلومات ( Down- load ). وهنا يتساءل بعضهم هل بإستطاعة التقنية الحديثة أن تزود المستفيدين بالمعلومات التي كان المهني يساهم في إيصالها؟ وعلى الجانب الآخر إذا استطاع المستفيد أن يتزود بمهارات البحث التقني فهل يترتب على ذلك تضيق الفجوة بين المستفيد والمهني؟ أعتقد أن الإجابة تفرض نفسها لأن الأمية الحاسوبية ( Computer Illiteracy ) مازالت

---

(1) الموقع السابق.

تسيطر على معظم المستخدمين، ولا أهين نكاعكم إذ أوضح معنى الأمية الحاسوبية، فليس القصد منها هو عدم القدرة على تشغيل الحاسب ولكن هو القدرة على البحث المحترف على الحاسب وحتى على أوعية المعلومات التقليدية المقروءة والمرئية والمسموعة. فالأمية الحاسوبية قد تخرج من تحت عباءة الأمية المعلوماتية ( information Illiteracy ) التي تعني عدم قدرة الفرد على استخدام المعلومات ومصادرها خصوصاً في ظل التعقيد المتزايد والمترامك لمخرجات الإنتاج الفكري العالمي<sup>(١)</sup>.

**المؤشر الثاني:** يؤيد استمرارية احتفاظ المهني بدوره ومكانته مشيراً إلى أن الدور المنوط بالمكتبي يمثل حلقة وصل أو إن شئت قل طرفاً في معادلة لا يمكن تحقيق نتائج بدونه لأنه يمثل العلاقة المباشرة بين المستخدمين والمعلومات فعلية سبيل المثال نحن الآن في عام ٢٠٠٤ وفي ظل تراكم وتكدس المعلومات وقواعد البيانات مترامية الأطراف يأتيها الباحثون من أقصى الدولة إلى أقصاها وبجميع درجاتهم العلمية إلى دار الكتب ( National Library ) يعنيه معلومات بعينها هذه المعلومات بالطبع لا تجلبها إلا خبرة سابقة ولا تعالجها إلا ممارسة حية على دراية بكل أوعية المعلومات التقليدية وغير التقليدية.

لقد تغيرت مهام ووظائف أمين المكتبة الإلكترونية من أداء الوظائف التقليدية إلى مهام استشاري معلومات، ومدير معلومات، وموجه أبحاث، ووسيط معلومات للقيام بعمليات معالجة المعلومات وتفسيرها وترجمتها وتحليلها، وإتقان مهارات الاتصال للإجابة على أسئلة المستخدمين، وكذلك الارتباط ببنوك وشبكات المعلومات وممارسة تدريب المستخدمين على استخدام النظم والشبكات المتطورة، وتسهيل مهمات الباحثين. ويرى بعض

---

(١) لموقع السابق.

الخبراء والباحثين أن المكتبة الإلكترونية ستزيد الطلب على اختصاصي المعلومات من أصحاب الخبرة والمعرفة الواسعة للقيام بالمهام الآتية:

١- استشارى معلومات يعمل على مساعدة المستخدمين وتوجيههم إلى بنوك ومصادر معلومات أكثر استجابة لاحتياجاتهم.

٢- تدريب المستخدمين على استخدام المصادر والنظم الإلكترونية.

٣- تحليل المعلومات وتقديمها للمستخدمين.

٤- إنشاء ملفات بحث وتقديمها عند الطلب للباحثين والدارسين.

٥- مساعدة المستخدم فى استثمار شبكة الانترنت وقدراتها الضخمة فى الحصول على المعلومات.

ومثل هذه المهام تتطلب إعداداً خاصاً لاكتساب مهارات معينة فى مواجهة التطورات السريعة والمذهلة فى تكنولوجيا المعلومات والاتصالات، وتقديم خدمات شاملة ومتجددة تتماشى مع روح العصر وثورة المعلومات. فضلاً عن ذلك فقد أسست جامعة كاليفورنيا فى بيركلي ( Berkely ) مدرسة نظم المعلومات ( SIMS )، وكانت رسالتها تتعلق بتكوين أمناء المعلومات الذين تتصل مهامهم بتنظيم ومعالجة وتنقيح وعرض المعلومات، ولا تقتصر وظيفتهم على إدارة التكنولوجيا فحسب، وإنما إدارة المعلومات والناس معاً.

ويذهب بعضهم إلى أن الوظيفة الأساسية التى يقوم بها أمين المكتبة الإلكترونية هى تحديد مكان المعلومة أو أماكنها، أو المعلومات المطلوبة منه سواء أكان طالب المعلومة رجل أعمال، أو شركة، أو باحثاً، وسواء أكانت المعلومة خاصة بمنافسة تجارية، أو تتعلق بدراسة موضوع علمي أو صناعي، أو تتعلق بتحديد خلفية بحثية لموضوع ما، ولتحقيق ذلك يستخدم أمين هذه المكتبة جميع وسائل الاتصال الإلكترونية.



## حقوق الإنسان من المعلومات<sup>(١)</sup>:

هناك تخوف من تدني مؤشرات حقوق الإنسان من المعلومات خصوصاً في ظل هذه الأعاصير المتلاحقة لموجات التطور التقني لمعالجة المعلومات وياتت مؤسسات المعلومات تهتم بترويج المعلومة باعتبارها سلعة وليس باعتبارها خدمة ومن هذه المؤشرات:

١- الاتجاه نحو تركيز خدمات المعلومات في عدد من شركات تقنيات المعلومات التي تهتم بالربح في المقام الأول.

٢- تركيزها لدى الشركات التجارية بهذا الشكل قد يوفر أرضاً خصبة لضياع حقوق الفرد من المعلومات وذلك لحكرها على نوى اليسار مما يلحق الضرر بالفرد غنياً كان أو فقيراً.

٣- استفاضة المناطق الريفية ببطء وفي ذلك عدم عدالة في التوزيع بالمقارنة بالمناطق ذات الاهتمام البؤري التي تتركز فيها عناصر الخدمة، صحيح أن الاتصالات بعيدة المدى Telecommunications قد وفرت الكثير من الخدمات لمثل هذه المناطق النائية إلا أن لمثل هذه الأبعاد الكثير من الانتقادات.

٤- تسميط المعلومات، فالمعلومات على الخط المباشر أياً كانت طبيعة هذا الخط يسودها نمطية، هذه النمطية قد تكون أو هي بالفعل معدة سلفاً وتوجه بشكل متعمد، فعولمة اللغة الإنجليزية على مواقع الشبكة العنكبوتية ( www ) أمر متعمد وهي التي تمثل نصيب الأسد حوالي ٦٩% في عمليات البحث المعلوماتي المستدق، وهنا بالتحديد لا تبتعد الأهداف السياسية عن التدخل في هذا المجال لأن توجيه المعلومة ليس أقل من توجيه الصاروخ ففي النهاية إنما يوجه الصاروخ بالمعلومة.

---

(١) الموقع السابق.

٥- إن أغنياء المعلومات ربما يكونون دولاً أو مؤسسات وربما يكونون أفراداً أيضاً، لأن الفرد هنا يستطيع من محطة تشغيل واحدة أن يقوم بمئات الوظائف في مجالات جميع وتجهيز البيانات وبث ونشر المعلومات، مستعيناً في ذلك بمراسد المعلومات ووسائل الاتصال الوطنية والدولية جميعاً.

نحو استراتيجية عربية لمواءمة تقنيات المجتمع الرقمي الجديد:<sup>(١)</sup>  
كمطلب أول لاستشراف آفاق المستقبل نحو مجتمع المعلومات في الوطن العربي، ينبغي إعداد المجتمع العربي وفق ما يلي:

١- أول هذه الاعتبارات هي الإعداد لميزان عادل ومعياري موحد تقوم على أساسه كيفية تقويم أداء المكتبات العربية من خلال المعيار الكيفي والنوعي لا الكمي.

٢- اعتبار تهيئة المجتمع العربي لمتطلبات مجتمع المعلومات قضية ثقافية ذات أولوية أولى، باعتبار أن العصر المقبل هو عصر المعلومات.

٣- ثمة ضعف في الهياكل السياسية لتقنية المعلومات في معظم البلدان العربية سببه قلة المتخصصين وقلة الذين يؤهلون للمستقبل التقني المعلوماتي، يقابل ذلك أن الإنتاج المعرفي يتضخم في العالم بشكل يزيد على سرعة المتواليات الهندسية. حيث لابد من البدء الفوري بإعداد الهياكل المتخصصة اللازمة.

٤- من الأهمية بمكان مواجهة المشاكل المزمنة في تحقيق تكامل معلوماتي عربي نتيجة للحدود المغلقة وعدم وجود المؤسسات العربية بالسرعة التي تفرضها (الديناميكية) للثورة الإلكترونية.

٥- لابد من التركيز على الجانب التعليمي والتربوي وعدم الاكتفاء بالتعليم الرسمي، بل يجب أن يشمل ذلك التعليم الذاتي والتعليم المستمر

---

(1) لموقع السابق.

ومواكبة خطط التعليم لخطط التنمية، فالمخططون لعمليات التنمية لا يولون تقنية المعلومات أى اهتمام وخاصة فى التربية.

٦- ضرورة تغيير الفلسفة التعليمية من الأسلوب التقني الصرف إلى أسلوب يشجعه على تنمية قدرات حل المشكلات والملفات الابتكارية والفنية.

٧- دراسة واقع مرافق المعلومات العربية وتبادل الآراء حول سبل مواكبة التطورات الحاصلة فى مسائل إدارة المعرفة والجودة الشاملة.

٨- ضبط جودة خدمات المعلومات فى العصر الإلكتروني: قياس أداء المجموعات والإجراءات الفنية والخدمات الموجهة لجمهور المستفيدين كالأهتمام بالجودة الشاملة فى إدارة مؤسسات المعلومات فى الوطن العربي: من الحوافز والامتنياز والإنتاجية.

٩- وضع تشريعات حازمة لإلزام دور النشر والجامعات ومراكز الأبحاث برقمنة كل ما سبق ونشرته على الأقل خلال العشر سنوات السابقة.

١٠- ضرورة وجود جهة مسؤولة عن مشروع الرقمنة ومراقبتها.

#### الخلفية التاريخية لدعاوى الملكية الفكرية<sup>(١)</sup>:

##### \* دعاوى قديمة - جديدة:

قد يعتقد البعض - خطأ- إن دعاوى الملكية الفكرية حديثة ومستجدة، لكن الحقيقة أنها من الدعاوى القائمة منذ فجر القرن معتمدة على طائفة من التشريعات والاتفاقيات الدولية التى انطلقت مع نهايات القرن التاسع عشر، ففى الأردن مثلا- كما فى عدد من الدول العربية المجاورة- ظل قانون حق المؤلف العثماني ساريا اعتبارا من عام ١٩٠٦ إلى أن تدخلت الدول بوضع تشريعات أكثر شمولية فى ضوء موجبات الاتفاقيات الدولية التى تديرها المنظمة العالمية للملكية الفكرية- الويبو- (وعندها لالن ٢١ اتفاقية) إلى

(1) لموقع السابق.

جانب اتفاقيتين لم تنفذا بعد في حق حق المؤلف والحقوق المجاورة. وفي عدد من الدول العربية - كالأردن مثلا تم إلغاء قانون حق التأليف العثماني واستبداله بتشريعات حماية حق المؤلف وشهدت التسعينات موجة تشريعية واسعة في المنطقة العربية أبرز ملامحها إضافة برامج الكمبيوتر وقواعد البيانات إلى نطاق المصنفات محل الحماية بموجب تشريع حق المؤلف.

وأنصبت الدعاوى في السنوات بل العقود السابقة على حماية أصحاب الإنتاج المعرفي وتجديدا في حق الكتب والمصنفات الفنية، وحملت تلك الدعاوى في نطاقها نكهة الدفاع عن المبدع العربي في موطنه العربي ضد الأنشطة التي تمثل اعتداء على نتاج عقله من الكتب ومختلف مصنفات الأديب والفن ولم تلبث ان انطفت جذوة هذه الدعاوى لسبب حقيقي واحد وهو أن قرصنة مثل هذه المصنفات لم يعد بالعمل المجدي لمركبه إذا ما انتهج الطريق القانوني الفويم، بل إن المستخدم لم يعد يتقبل النسخ المقلدة أو المصورة أو المستنسخة من المصنفات مادام سعر الأصل يقارب أن لم يكن أقل من سعر المستنسخ، بمعنى أن استراتيجيات التسعير والتسويق ساهمت وحدها بمحاربة نشاط القرصنة في حق الكتاب، مع بقاء استثناءات محصورة في حق الكتب الأكاديمية وتجارتها التي جاء القانون ليحد منها من خلال وسيلة الترخيص الإجباري الممنوح للسلطة الحكومية حفاظا على الاحتياجات الثقافية والعلمية. والنتيجة أن الواقع العربي لم يشهد الكثير من دعاوى الملكية الفكرية على مدى سنوات، ولا نبالغ أن قلنا أن القوانين العربية في هذا الحقل لم تمتحن جميعها في التطبيق لغياب المنازعات في هذا الحقل.

\* انطلاقاً عصر تحرير الخدمات والتوجه للاقتصاد الرقمي يعيد جذوة دعاوى الملكية الفكرية: (١)

بالرغم من انطلاق الجهد الدولي المنظم في حق تحرير التجارة منذ عام ١٩٤٧ الذي شهد ولادة اتفاقيات الجات، إلا أن تحرير التجارة في السلع بقي يواجه معقبات كبرى أهمها عدم قبول الولايات المتحدة طائفة كبيرة من اتفاقيات تحرير التجارة برغم من الجولات التفاوضية السبعة التي سبقت جولة الأورغواي ( ١٩٨٦ - ١٩٩٤ )، وفي جولة الأورغواي للتفاوض بشأن تحرير التجارة في السلع، انتقل العالم إلى واقع جديد حين فاجأته الولايات المتحدة بقبول غالبية ما كانت ترفضه من اتفاقيات في حق تجارة البضائع، ولم يكن هذا الموقف خالياً من رؤية استراتيجية للمصالح الأمريكية في المستقبل، بل هو وليد دراسات وتخطيط استراتيجي ساهمت فيه مختلف الشركات العملاقة متعددة الجنسيات، حيث اقحمت القوى الغربية في جولة الأورغواي - برغم معارضة الدول النامية - موضوع الملكية الفكرية ( اتفاقية ترينس ) وموضوع تحرير التجارة في الخدمات، لجهة خلق واقع جديد يتيح لمالكي المعرفة والكفاءة الاستفادة من كافة الأسواق العالمية وتعزيز استثماراتهم فيها، وفعلًا تحقق هذا الهدف بإقرار اتفاقية ترينس بشأن الملكية الفكرية ليخلق لأول مرة منذ أكثر من مائة عام مركز آخر للملكية الفكرية غير المنظمة العالمية ( الوايو ) ولتصبح اتفاقية ترينس الإطار الأكثر شمولية لمعالجة كافة مسائل الملكية الفكرية. وأقرت أيضاً اتفاقية تحرير الخدمات (جاس) التي تتيح لمقدمي الخدمة تعاملًا مماثلاً للجهات الوطنية في الدولة وترفع من أمامهم معيقات الوصول للأسواق الخارجية. وفي هذا الإطار كان يتعين على كل دولة ترغب بعضوية المنظمة أن تقبل هذه الاتفاقيات التي

(1) <http://arabia.bitsnips.com/forums/viewtopic.php?p=249&sid=8d5440aeaacc2e02188c887..>

تفرض التزامات تنظيمية وتشريعية من بينها أن تتواءم تشريعاتها في حق الملكية الفكرية مع اتفاقية ترينس. وفي هذا الإطار شهدت الدول العربية موجة واسعة من تعديل التشريعات القائمة أو وضع تشريعات جديدة، وأحدثت ثورة حقيقية في النظام القانوني للملكية الفكرية في الوطن العربي لا تزال ملامحها غير واضحة، فإذا كانت الخطط المعلنة هي تعزيز الملكية الفكرية لاستجلاب الاستثمار الأجنبي باعتبار ذلك من الأمور المرغوبة لجهات الاستثمار وأحيانا من مطالبها، فإن حركة الاستثمارات الأجنبية في الأسواق العربية لا تشير إلى تحقق هذا الغرض بالرغم من أن دولا عربية أقرت تشريعات تحمي الملكية الفكرية أكثر نضجا وشمولية مما هو قائم في دول أجنبية. وبنفس الوقت ظهرت في الواقع العملي ظاهرة نشاط الشركات الأجنبية لتنظيف الأسواق العربية مما يسمونه خطرا على استثماراتها ونقص ذلك ما يثار حول مخاطر القرصنة، ولم تكتف هذه الجهات بالخطط الحكومية الطموحة لتحقيق هذا الغرض، فباشرت بذاتها حملة نقاش- هي حق لها من الوجهة القانونية ومن وجهة نظر العدالة- مترافقة مع حملة تعديل التشريعات إلى المدى التي ظن البعض أننا أمام تشريعات جديدة وأن حماية برامج الحاسوب انطلقت مع هذه القوانين، مع أن الحماية مقرر منذ نحو عشرة سنوات.

#### النطاق القانوني لحماية برامج الكمبيوتر وقواعد البيانات في البيئة العربية<sup>(1)</sup>:

تتضمن قوانين حماية حق المؤلف العربية عموما النص على حماية الكتب والكتيبات وغيرها من المواد المكتوبة، والمصنفات التي تلقى شفاها كالمحاضرات والخطب والمواعظ، والمصنفات المسرحية والمسرحيات

---

(1) لموقع السابق.

الغنائية والموسيقية والتمثيل الإيمائي، والمصنفات الموسيقية، والمصنفات السينمائية والاذاعية السمعية والبصرية، وأعمال الرسم والتصوير والنحت والحفر والعمارة والفنون التطبيقية والزخرفية، والصور التوضيحية والخرائط والتصميمات والمخططات والأعمال المجسمة المتعلقة بالجغرافيا والخرائط السطحية للأرض، وبرامج الحاسوب ( كما في طائفة منها) وفي أعقاب سريان اتفاقية ترينس في عدد من الدول العربية أصبحت الحماية تمتد إلى البرمجيات سواء كانت بلغة المصدر أو الآلة، إضافة إلى حماية ما يمكن أن يسمى قواعد المعلومات المجمعة وتحديدًا حماية طريقة التجميع سواء أكانت بطريقة تقليدية أم آلية ( قواعد البيانات). وذلك للتوافق مع متطلبات المادة ١٠ من اتفاقية ترينس العالمية ( اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية).

وتحمي برامج الحاسوب وقواعد البيانات وفقًا لقوانين حق المؤلف- بوجه عام - طيلة حياة المؤلف ولمدة خمسين عاما بعد وفاته، ويوجه خبراء التقنية والقانون الدولييين انتقادا لمدة الحماية هذه باعتبارها طويلة لا تتناسب مع الطبيعة المتغيرة والمتسارعة للبرمجيات واستغلالها لمدد قصيرة، أما إذ كان مالك حقوق المؤلف شخصا معنويا- وهو الفرض الغالب بالنسبة للبرمجيات، فإن مدة الحماية تقل عن مدة حماية حقوق الأشخاص الطبيعيين كما في عدد من قوانين الدول العربية<sup>(١)</sup>.

وتشمل الحماية الحقوق المعنوية للمؤلف والحقوق المالية لاستغلال المصنف وهي حماية استثنائية للمؤلف وحده يمنع بموجبها أى استغلال أو استعمال يضر بمصلحة المؤلف، وتعطي للمؤلف وحده الحق في استنساخ مصنفه وإجازة استعماله، وفقا لشروط تقررها القوانين العربية في هذا الحقل

---

(١) الموقع السابق.

تتصل بمباشرة حقوق المؤلف ونطاق الاستغلال ومحتواه، تنص القوانين أيضا- على تبين بيها- على استثناءات معينة ترد على مباشرة حقوق المؤلف، ولا تعد من قبيل التعدي، مثالها إجازة استخدام المصنف دون إذن المؤلف أو مالك الحق في معرض تقديم المصنف عرضا أو القاء خلال اجتماع عائلي أو في مؤسسة تعليمية أو ثقافية أو اجتماعية على سبيل التوضيح أو الاستعانة بالمصنف لأغراض شخصية بعمل نسخة واحدة دون تعارض مع الاستغلال العادي، واستعماله في الإيضاح التعليمي والاستشهاد بفقرات منه في إنتاج ووضع مصنف آخر. ومن أكثر التحديات في حقل الاستثناءات مفهوم الاستعمال الشخصي للمصنف ومداه ونطاقه إضافة إلى الإشكالات المتصلة بمدى ونطاق الاستثناء الخاص باستخدام المصنفات لغايات علمية أو بحثية أو في معرض الاستعمال العارض<sup>(1)</sup>.

وتجيز بعض القوانين للسلطات إصدار أمر بالترخيص الإجمالي للمصنف الأجنبي رغما عن مالكه لجهة وإعادة إنتاجها وبيعها بالسعر المساوي لمثيلاتها في السوق أو السعر العادل ضمن ضوابط وشروط يراعي فيها تعويض مؤلف المصنف أو صاحب الحق عن هذا الترخيص الإجمالي. وتتبع الدول طريقة الترخيص الإجمالي حماية لاحتياجات المجتمع والعملية التعليمية، وتتباين المواقف حول نطاق الترخيص الإجمالي إذ يحدد القانون عادة المصنفات القابلة لمثل هذا الإجراء، وهو أيضا إجراء هام لمواجهة سياسات الاحتكار ومنعا للتحكم في رواج الفائدة المتوخاة من المصنف وبسبب الأثر الذي أحدثته اتفاقية ترينس، لم يعد شرط إيداع المصنفات مطلوبا لغايات الحماية القضائية، وهو ما أدى إلى تعديل عدد من تشريعات حق المؤلف العربية لتعكس هذا الحكم كما أن التشريعات الحديثة منها نصت أيضا على عدم اشتراط الإيداع.

(1) للموقع السابق.



\* محل الحماية<sup>(١)</sup>:

بالرجوع للدراسات المقارنة والتطبيقات القضائية الشهيرة يظهر أن تحديد مفهوم البرنامج ونطاقه خلق إشكاليات عديدة، أولها ما إذا كان إعادة إنتاج البرنامج باقتباس أجزاء منه، أو باستخدام طريقة الهندسة العكسية أو باتباع وسائل برمجية (معنوية) غير المتبعة في إنتاجه أصلاً، يعد من قبيل النسخ غير المشروع أو التقليد، ويتفق القضاء على أن التقليد أو النسخ لكامل المنتج بغرض الاستغلال المالي لا يثير إشكالا في التطبيق، لكن ما يثير الإشكال اقتباس الخوارزميات المحتواة ضمن البرنامج، ومرد ذلك أن القضاء الأجنبي في معرض نظره لدعاوى حقوق المؤلف على البرمجيات اتسق مع أحكام الاتفاقيات الدولية بشأن عدم شمول الخوارزميات والحقائق للحماية، وهذا ما يعني أن الاقتباس فيما لا يتجاوز النسخ الجزئي وطريق الهندسة العكسية المتبعة في إعادة بناء البرنامج تخضع لمعايير معينة قبل القول بحصول النسخ أو الاعتداء على حق المؤلف.

ويثور الإشكال أيضا بالنسبة لحماية لغة البرمجة، وتعديلات استخدام برامج التشغيل للتوافق مع بيانات العمل التقني أو لجهة إصلاح أخطائه، ومفهوم أن الشائع في حقل القرصنة بالعموم إنما هو برمجيات التشغيل الشهيرة وبرامج التطبيق الشائعة، لكن الإشكال يثور حول النسخ التجريبية التي يزود بها المستخدمون، فهي ليست المصنف النهائي المثبت ملكيته، ويثبت ذلك بالمعايير الفحصية عبر الخبرة، ومعلوم أن الشائع والسائد في الدول النامية النسخ التجريبية التي يتلقاها في وقتنا الحاضر معظم المستخدمون عبر شبكة الإنترنت أو حتى من بائع الأجهزة بحصوله عليها

---

(1) الموقع السابق.

من الوسائط التي تملأ العالم ضمن سياسات الترويج الإعلامي التي اتبعتها وتتبعها المؤسسات المنتجة للبرمجيات. وفي هذا الصدد تشير إلي أن عددا من الدعاوى قد أقيمت علي عدد من المحال بخصوص الألعاب الإلكترونية، وأن عددا من هذه الدعاوى قد استند إلي ضبط برمجيات تتضمن ألعابا غير مصرح ببيعها ليتبين بالخبرة الفنية وأحيانا (تغيب هذه الحقيقة) أن هذه البرمجيات لا تضم أكثر من نسخة دعائية للعبة أو (ديمو) مصغر أو نسخي تجريبية، مما ينفي ارتكاب المخالفة لقانون حق المؤلف، باعتبار أن الشركات الأجنبية تروج طويلا لمنتجاتها قبل طرحها فعليا في الأسواق، وغياب المعرفة التقنية وحقائق البرمجيات يستغل من البعض في الإيهام بأن النسخ التجريبية أو الدعائية نسخ مقرصنة، وهذه مسألة لا تحسمها غير الخبرة المؤهلة، لا في حقل التقنية فقط، بل في حقل الأعمال وتجارة سوق التقنية التي تتطلب علي سياسات واستراتيجيات يتعين علي جهات الخبرة والقضاء والمحاماة معرفتها سيما أنها أصبحت في متناول اليد من خلال مواقع هذه الشركات علي شبكة الإنترنت.

**\* شرط ملكية الحق أساس الدعوى ولا دعوى دون توفر الصفة في التقاضي<sup>(1)</sup>:**

أن حماية أي المصنف توجب أن يثبت الحق بملكيته لطالب الحماية، سواء تعلق إجراء الحماية بالمطالبة المدنية (الدعوى المدنية يشقيها الموضوعي والطلبات المستعجلة) أو الدعوى الجزائية (الشكوى) أو الإجراء الإداري عبر مكتب الحماية. وشرط ثبوت تملك الحق المعنوي أو حق الاستغلال المالي، شرط مصلحة وصفة، بل أنه ابتداء عنصر رئيس لتفعيل عمل نصوص الحماية، بمعنى أنه الشرط الموجب لقبول الدعوى، فلا دعوى

---

(1) لموقع السابق.

دون أن ثبت زاعم الاعتداء أنه المالك الحقيقي والقانوني لحقوق المؤلف علي المصنف، وهذه من أكثر الإشكالات التي تواجه دعاوى الملكية الفكرية في الساحة العربية، فالإيداع لم يعد مطلباً وفقاً لاتفاقية ترينس وقد اعتقدت العديد من الجهات أن ذلك يعفيها من إثبات الملكية أو أنها جهات شهيرة إلى مدى يعرف القاضي أنها المالكة للحق علي برنامج ما، وهذا ليس صحيحاً، إذ علي فرض صحته فإن القاضي لا يحكم بعمله عوضاً عن أن مباشرة حقوق حماية المصنف تتطلب أن تتم ويتم فقط من المؤلف وحده الذي منح حق الدفاع عن مصنفه، وتصبح المشكلة أكثر تعقيداً عندما يتصدى لرفع الدعوى وكيل عن مالك الحق، وما لم تثبت وكالته القانونية أنه وكيل بالخصومة وينوع هذه الخصومة فإنه لا وجه لقبول الدعوى ابتداءً. ويشترط أن يثبت ملكية حق الخصومة والتقاضى لمن يباشر دعوى أو طلب الحماية عندما لا يكون هو المؤلف أو المتنازل إليه من المؤلف مباشرة عن حق الاستغلال المالي، أما إذا كان المتنازل إليه من المؤلف مباشرة عن حق الاستغلال المالي، أما إذا كان طالب الحماية بالإجراء المعين وكيلاً أو موزعاً فإنه لا يملك غير المقاضاة المدنية بما تعرض له هو بصفته هذه، لا بما تعرض له مؤلف المصنف أو مالك الحق فيه، لأن نطاق وصحة المطالبة تتحدد بسببها، فلن امتد سبب المطالبة إلي إدعاء الاعتداء علي حق المؤلف فهو - أي المؤلف وحده - من يحمي الحق أو من يحق أن يوكل غيره في الخصومة القضائية لهذه الغاية تحديداً، وكل ذلك مرهون بنصوص عقود واتفاقيات الوكالة والرخص، وهو ما يدعونا في هذا المقام للتنبيه إلي أن كثيراً من المؤسسات كانت محللاً لتعاقدات غير عادلة مع الأطراف الأجنبية بسبب عوامل كثيرة أهمها مدى كفاءة المفاوض وعدم توفر المشورة القانونية المؤهلة المتخصصة في هذا الحقل الهام.

• مرخص أم غير مرخص - أكثر الحقائق الغائبة<sup>(١)</sup>:

لقد وقعت العديد من الشركات والمؤسسات العربية ضمن نطاق تأثير الموزعين والوكلاء بل وسماصرة السوق، وتعرضوا للإيهام بأن أوضاعهم القانونية مخالفة للقانون مع أن وضعهم القانوني قد يكون سليماً ولا غبار عليه، ومثال ذلك اعتبار مؤسسة ما غير مرخصة مع أنها تملك أجهزة حواسي ذات ماركات عالمية منتجة من شركات عقدت اتفاقيات داخلية مع جهات إنتاج البرامج تعتبر بموجبها أجهزتها مرخصة حكماً حتى لو لم تتحقق معايير الترخيص المقررة لدى جهة إنتاج البرامج. ومثال آخر اعتبار حائز التسجيلات التي سبق له شراؤها من أحد الوكلاء السابقين مخالف للقانون لأن وكالة الوكيل التجارية تحظر عليه إبقاء أي مخزون لدى التجار في نهاية مدة وکالته، فيخل بالتزامه ويعرض للتجار للمسئولية أمام الوكيل الجديد الذي لا يفترض غير أن التاجر قد نسخ مصنفاته دون إذن، ومثال ثالث استغلال عدم معرفة العديد من المؤسسات بأنها مرخصة أصلاً لعدم معرفتها بماهية الرخصة ذاتها، وأشير في هذا المقام إلى أن الأسواق العربية تشيع فيه ممارسات من قبل بائعي الأجهزة التقنية (مارسات السوق) من ضمنها مثلاً تنزيل نسخة واحدة من البرنامج عن قرص واحد على عدد من الأجهزة رغم أن المشتري كان قد اشترى عدداً من البرمجيات المرخصة يساوي عدد الأجهزة، بحيث تظهر كافة الأجهزة محملة بنفس رقم البرنامج فتتعرض لاتهمها بنسخ البرنامج على أجهزتها مع أن الواقع غير ذلك. ومن الممارسات أيضاً عدم إرسال كتيب الرخص من قبل البائع على اعتبار أنه كتيب تعليمات لتستأجراً الشركة بعد ذلك أنها غير مرخصة لأنها لم تحضر رخص برمجياتها من البائع الذي يكون قد أودعها مخزنة أو مستودعا ما أو ربما اعتبرها من مخالفات الأجهزة كعبوات التغليف والكتيبات فألقاها أو ألقاها إلى حيث يلقي

(١) لموقع «سابق».

مخالفاته غير الهامة. ومثل هذه الممارسة قد تتم من الشركة المشترية التي لا تعير الكتيبات والأدلة والأوراق المصاحبة للجهاز اهتماما كافيا أو لا تعير أهمية للاحتفاظ بالرخص في موضع يمنع فقدانها وضياها.

ومن المخاطر الحقيقية لعدم الوعي السائد بشأن التراخيص استغلال البعض لهذه الممارسات التي لا دخل للمستخدمين بها بسبب غياب المعايير والمواصفات التقنية وغياب استراتيجيات تنظيم السوق التقني في البيئة العربية، وأوضح مثال علي ذلك أن بعض الجهات التقنية تعتبر المستخدم غير مرخص لاستخدام برنامج معين حتى لو أبرز الرخصة المطابقة نوعا وتاريخا للبرنامج لكنها لا تتطابق مع البرنامج من حيث رقم المنتج، إذ قد يختلف رقم البرنامج الموجود علي الجهاز مع رقم المنتج الوارد علي الرخصة لأسباب كثيرة، منها- كما ذكرنا- أن بعض الجهات تقوم بإنزال البرنامج علي عدة أجهزة عن قرص واحد لتوفر وقت إنزال كل برنامج من القرص الخاص به وباعتبارها جميعا نسخا متطابقة عن البرنامج. أو قد يتم محو القرص الصلب بكامله لغايات الصيانة أو التطوير فلا تراعي جهة الصيانة تنزيل النسخة الموجودة عند العميل وتنزل من طرفها نسخة عن ذات البرنامج فيختلف الرقم، وقد يختلف الرقم لأي سبب آخر باعتباره من الناحية التقنية قابل للتغيير بتدخل شخصي أو نتيجة عمليات مؤتممة مما يجعل الرقم مغايرا للرقم الموجود علي الرخصة، وهذا لا يعني أن المستخدم غير مرخص له باستخدام البرنامج، لأن رقم المنتج ليس معيارا للترخيص غير مرخص له باستخدام البرنامج، لأن رقم المنتج ليس معيارا للترخيص ولا هو مطلب له، والمعيار فقط توفر وثيقة الرخصة ذاتها المطابقة للبرنامج نوعا وتاريخا فقط، إذ لا يعتد بما يقبل التغيير كالرقم ولا أهمية له ولا دور يقوم به من ناحية الترخيص، وهو موجود فقط لتسهيل عمليات الدعم والصيانة (المسجلين لدى الشركة المنتجة فقط مع الإشارة إلي أن التسجيل اختياري

وليس متطلبات قانونيا لصحة الاستخدام) أو يستخدم الرقم داخل المنشأة لغايات التوثيق وصرف العهدة علي المستخدمين عند تعددهم.

لهذه الممارسات التي نشأت عن تشوه سوق التقنية وغياب المعايير والمواصفات علي مدى السنوات السابقة، علينا جميعا أن نعيد التفكير بشعار مكافحة القرصنة الذي يتعين أن يسبقه معرفة حقيقية وسليمة بالواقع المعاش وباستراتيجيات جهات الترخيص والإنتاج، فمن مصلحة المنتج أن يعتبر أي فعل من قبيل الاعتداء علي فرص ربحه، لكن من حقنا أيضا أن نعرف ما إذا كان فعلا يعتمد علي استراتيجية تتفق والقانون القائم، أم أنه يتحدث عن نظامه القانوني واستراتيجياته التي يرغب أن تكون قانونا لكنه لا يملك ذلك في ظل اعتبارات السيادة الوطنية<sup>(1)</sup>.

أن الاتفاقيات الدولية وبقدر ما منحت المبدع حقوقا علي نتائج إبداعه بقدر ما حمت المستهلك من التضليل والإيهام، وعلينا أن ندرك أن إيفاءنا بالتزاماتنا تجاه الغير - وهو أمر مطلوب ومرغوب لدينا بسبب التركيبة الاجتماعية والثقافية السائدة في مجتمعنا- يتعين أن يرافقه تمسكنا بحقوقنا التي نتطلق أولا من المعرفة والوعي بالحدود الفاصلة بين الحق والالتزام في هذا الحق.

أن الموضوعية تقتضي منا الإشهاد العالية باتجاهات القضاء في هذا الحقل، حيث أظهرت بعض الوقائع العملية أن القضاء يعتمد علي نفسه أولا وعلي خيرات فنية يقلبها بعناية للوصول إلي الحقيقة، ففي قرار صادر عن محكمة الاستئناف الأردنية (محكمة استئناف عمان في الدعوى رقم ١٣١٣/٢٠٠٠ تاريخ ٢٠٠٠/٥/١٨) بوصفها المرجع القضائي الأخير للطلبات المستعجلة قضى فيه ببطلان ضبط تسجيلات صوتية، قررت المحكمة إخضاع كافة الضوابط في ميدان الملكية الفكرية إلي شرائط القانون والحكم

---

(1) لموقع السابق.

بعدم قبول أي ضبط دون خبرة قاطعة بحصول السلوك الجرمي من الشخص المنسوب إليه الفعل بذاته، وينظر القضاء للأمر بكل عناية وموضوعية، وقد أظهرت الدعاوى المنظورة وعدد من المفصلة حتى الآن اتجاهها قضائيا يقوم علي تمحيص الحقائق إلي أبعد مدى لتبين الحقائق حول التراخيص مبرها في ظل تنوعها وفي ظل ما يعلن علي الملأ من إمكان الترخيص اللاحق للبرامج القائمة، بل في ظل صفقات الترخيص المسماة (التراخيص مع متطلبات القانون) فهي- ونحن لسنا ضدها علي الإطلاق بل تشجيعها- تثير من الوجهة القانونية التساؤل حول بعض الخبرات الفنية التي لا تقبل تراخيص بزعم مخالفتها لمعايير مقررلة لدى جهات الترخيص التي هي الشركات الأجنبية المنتجة ذاتها، كالمغايرة بين رقم الرخصة والبرنامج مع أنه غير متطلب ابتداء، والأساس- كما ذكرنا- التطابق بين الرخصة ونوع البرنامج وتاريخ تنزيله، فجهات الترخيص عند عقد الصفقات تكيف معاييرها لتمرير صفقاتها التجارية، لكنها في ساحات القضاء قد تتمسك بمعاييرها هي لضمان مركز أفضل أمام القضاء، ومن هنا فإن كافة الخبراء الفنيين العرب مدعوون للتعامل الدقيق والحذر مع الحالات المكلفين بها، لأن العلم لا يقبل التطويع لحساب سياسات نفعية، والقضاء يبذل كل جهد للوصول إلي الحقائق الموضوعية، ولأن كثيرا من المفاهيم تغيب في أوقات يفترض أن لا تغيب، وكثير مما يعتقد أنه حقيقة علمية لا يعدو مجرد سياسة تسويقية لشركة مستفيدة أو منتفعة.

وفي ميدان البرمجيات، تثار مشكلة نطاق التراخيص وحجبتها وأنواعها المستجدة، إذ لم تقف تراخيص التصرف بالبرمجيات واستعمالها عند حد الرخصة المكتوبة الموقعة من طرفها، بل أصبحت البرمجيات تباع كحزم جاهزة في أماكن البيع العام، تتضمن رخصا نموذجية غير موقع عليها، توجب التزام مشتري البرنامج بشرائطها بمجرد فض العبوة ونزع الغلاف،

كما أن من البرامج وتحديدًا تلك المشتراة علي الخط أو المنزلة والمثبتة عبر الشبكات كالإنترنت والإنترنت الخاصة بتسويق البرمجيات ما ترتبط فيها الرخصة بقبول الشروط المكتوبة والمنشورة علي الموقع بحيث يصبح الشخص ملزماً بمحتواها بمجرد القبول وأحياناً الاستعمال، وبعضها تتضمن الرخصة بشكل إلكتروني ضمن مقدمة البرنامج ذاته، مع مرافقة ذلك بإجراءات تسجيل يتم أحياناً بشكل مادي علي مستنداتها أو بشكل إلكتروني عبر الشبكة، ولا يترتب علي عدم القيام بها في حالات عديدة آثار علي صحة الاستخدام في حين أن شروط بعض الرخص تربط صحة الاستخدام بإتمام التسجيل وهذه الرخص تثير إشكاليات قانونية في التطبيق توجب التدقيق في طبيعتها والبت بأمر حجيتها في ضوء أحكام قانون البيانات وتحديده للأئمة المقبولة قانوناً<sup>(1)</sup>.

إن مشكلات عدم الإطلاع فعلياً علي هذه الشروط في كثير من الحالات مشكلات عدم معرفة قواعد الإثبات القائمة لهذه الشروط المخزنة داخل النظم كشروط نموذجية تثبت عناصر والتزامات التعاقد، لعدم التوقيع عليها وعدم ثبوت توجبها لشخص بعينه، وثبوت عدم مناقشتها بين الأطراف كل ذلك وغيره استوجب التدخل التشريعي لتنظيم آلية إبرام العقد التقني أو شروط حجيته وموثوقيته، سواء نتحدث عن العقد المتصل بالمبيع أو عن رخص الاستخدام بوصفها التزاماً بين جهتين.

وتثور أيضاً مشكلة رخص الملكية الفكرية المغلفة مع المبيع، وكذلك، حقوق الملكية الفكرية في ميدان النشر الإلكتروني خصوصاً مع تزايد الاستيلاء علي التصاميم التي يستخدمها موقع ما، وحقوق الملكية الفكرية علي أسماء المواقع، وعلي ملكية الموقع نفسه، وحقوق الملكية الفكرية

---

(1) لموقع سابق.



بالنسبة للعلامات التجارية للسلع، والأسماء التجارية، وكذلك حقوق المؤلفين علي محتوى البرمجيات التقنية التي تنزل علي الخط أو تسوق عبر مواقع التجارة الإلكترونية، أن كل هذه المشكلات التي ضاعفت سطوتها التجارة الإلكترونية استلزمت مراجعة شاملة للقواعد القانونية الخاصة بالملكية الفكرية وربطها بالأنشطة التجارية الدولية في ميدان البضائع والخدمات، وهي المبرر أيضا لإقرار اتفاقية تريس العالمية كواحدة من اتفاقيات منظمة التجارة الدولية التي تلتزم بها الدول الأعضاء، ولا تضيف جديدا إذا قلنا أن العديد من الدول ارتجلت قواعد في ميدان الملكية الفكرية دون النظر إلي متطلبات التجارة الإلكترونية، وهو ما جعل قواعدها، رغم حداثة تشريعها ووضعها، غير متوائمة مع متطلبات التجارة الإلكترونية<sup>(١)</sup>.

ومن بين مشكلات البت بمشروعية الاستخدام، حالة الترخيص باستعمال برنامج ما لمؤسسة أو جهة ومن ثم استخدامه من قبل عدد آخر من المستخدمين، أو استخدامه ضمن نظام يرتبط بشبكة بين شركاء أو حلفاء المستخدم أو ربما موظفيه عندما تكون الأعمال مدارة عبر شبكة إنترنت خاصة ضمن مفهوم وسياسة الأعمال الإلكترونية، ومثل هذه المشكلات تحدها طبيعة الرخص ذاتها ما إذا كانت لمستخدم واحد متصلة بشخصه- وليس بعدد أجهزته أم لجهاز واحد أم رخصة جماعية- وهي علي أنواع متعددة- كما في رخصة الموقع أو رخصة المؤسسة، ومن المهم هنا القول أن الرخصة تظل أيضا من العقود التي تخضع لقواعد التفسير، فإن كان المستخدم يلجأ لقواعد القانون للحصول علي أفضل مركز لدفاعه، فإن مانح حق الترخيص أيضا يلجأ لذات القواعد لتحقيق أفضل مركز وإثبات حصول الاستخدام غير المشروع.

---

(1) لموقع السابق.

ومن بين إشكاليات الترخيص، يتطلب حصول المستخدم وإثباته رخصة استخدام كل نسخة من نظام التشغيل حتى لو كان النظام قد خضع لتغيير لغة التطبيق (عبر برنامج الترجمة التقني) وهذا أمر حل نظر باعتبار أن البرنامج لدى حمايته في بلد المنتج أو الحماية الدولية له وفقا لنظام الحماية الذي اختاره صاحب الحق، قد لا يكون أكثر من تحديد للمنتج باسمه التجاري وطبيعته، وبالتالي فإن الحصول على هذا الترخيص يتضمن ترخيص كل تطوير له وكل استخدام لذات البرنامج بعد خضوعه للترجمة في بيئة الاستخدام، وبالتالي لا تمتد الحماية للبرنامج المترجم ما لم يكن بلغته المستخدمة محلا للحماية ابتداء ومسجلا بهذه الصفة.

أن أبرز مشكلات التعامل مع الرخص غياب المعرفة بأنماطها وتحديد مدى الصحة من عدمه ولعل هذا ما دعا مختلف الدول العربية لعقد عشرات البرامج التوعوية والتدريبية في حق الترخيص، وقد أظهرت هذه البرامج حقائق مذهلة حتى بالنسبة للخبراء الذين لم يسبق لهم معرفتها، وهذا يضع مجتمعنا وكل الجهات العاملة في حق الملكية الفكرية تحد علينا تجاوزه بكل فعالية، وهو التأهيل الصحيح البعيد عن الغرض لموضوع التراخيص منطلقين من حاجة الوطن ومؤسسات لبناء نظام تراخيص تفاوضي ومعرفي وقانوني وتنظيمي فيه الصالح الوطني عمادا وعنوانا.

• ثبوت أركان الجرم على نحو ما حدده القانون فقط وببديل مشروع<sup>(1)</sup>:

مما يثار في حق إشكالات الدعاوى الجزائية المتعلقة بالملكية الفكرية، المفاهيم العامة التي تطلق في الاتهام أحيانا وحتى في الدفاع من قبل بعض جهات الدفاع، كالقول أن الدعوى تقوم على فعل مخالف لقانون حق المؤلف في حين أن القانون الجزائي لا يعمل وفي هذه العمومية المفروضة بموجب

---

(1) لموقع السابق.

مبدأ المشروعية، وإلا لكنا نحيل السارق والقاتل والمزور بتهمة واحدة وهي مخالفة قانون العقوبات.

إن دعاوى المساءلة الجزائية في حقل الملكية الفكرية، تخضع شأنها شأن غيرها لقواعد المشروعية الجنائية، ويتعين أن تثبت عناصر الجرم وفقا لنموذجه القانوني فقط، وتخضع أيضا من حيث إثبات المسؤولية لمبدأ مشروعية الدليل من حيث مصدره وانتفاء احتمالات الشبهة والغاية فيمن يعتمد عليه لإثبات الجرم. ولا تثبت كافة العناصر وكذا لا تقبل الأدلة علي سبيل الاحتمال، وإنما علي سبيل الجزم واليقين شأنها شأن غيرها من الدعاوى الجزائية، ويتعين أن يحدد مرتكبها دون شك، لأن المسؤولية الجزائية شخصية، ولأن نطاق مسؤولية الأشخاص المعنوية توجب إثبات قيام ممثل الشخص المعنوي قانونا أو من في حكمه بارتكاب الجرم المتوفر فيه كافة الأركان المقررة قانونا، المادي والمعنوي ووفق النموذج القانوني المحدد في نص التجريم<sup>(١)</sup>.

أن القضاء المقارن قد قرر وجوب ثبوت تحقق الاستمساخ أو التقليد بمعني ثبوت مقارفة السلوك المادي المكون للجريمة وفق ما نص عليها القانون، وبشكل لا يظهر منه أن محل النسخ واحدة من عمليات الاقتباس أو ما عرف بنسق الهندسة العكسية في بيئة إنتاج البرمجيات، وهذه مسائل تتطلب الخبرة القانونية والفنية، وهي لجنتها في ميدان النقاضي تثير عشرات الدفوع والمسائل الفرعية التي سيكون للخبرة فيها دورا حاسما وأساسيا، مع التأكيد أن الخبير الأعلى إنما هو القاضي، وهو الذي يحكم في المواد الجزائية بقناعته الذاتية ووجدانه المستقي والمستخلص علي نحو سائغ من أدلة الدعوى.

---

(1) الموقع السابق.

أن محكمة الاستئناف الأردنية وفي أحدث أحكامها (الدعوى الاستئنافية رقم ٢٠٠١/٢٠١ الصادر قرارها بتاريخ ٢٠٠١/٢/٢١) في ميدان دعاوى المسؤولية عن قرصنة برامج الكمبيوتر، خللت بكل دقة وعمق النصوص الجنائية المقررة في قانون حق المؤلف الأردني، وتوصلت بوضوح إلى أن الأنشطة المجرمة في هذا الحقل تنحصر بأنشطة الاستغلال المالي المتمثلة بالعرض للبيع أو التأجير وفي حدود غرض محدد فقط وهو الاستغلال المالي ومن هنا قررت بوضوح أن الاستخدام دون الاستغلال المالي لا يعد جرماً وفق قانوننا، وأنهت نهاية موضوعية وعادلة واحدة من دعاوى الملكية الفكرية التي طالت واحدة من المؤسسات المالية الكبرى، ولا نبالغ أن قلنا أن حماية الإبداع بكل صوره في ميدان الملكية الأدبية والصناعية قام على أساس الموازنة بين احتياجات المبدع لصيانة إبداعه ومنحه الفرصة (المؤقتة بمدة معينة) لاستثمار نتاج عقله، وبين حاجة المجتمع للمعرفة ووسائلها، هذه الموازنة التي تمنع احتكار صاحب المصنف لمصنفه وتجيئ ترخيصه إجبارياً لحماية الثقافة وتلبية احتياجات التنمية والتطور في المجتمع، وإذا كان من حق مالك حقوق أي مصنف أن يحمي إبداعه، فإن من حق مجتمعنا علينا أن لا تكون هذه الحماية على نحو يمس عناصر تطوره ويخل بميزان التناسب بين الحماية الخاصة والاحتياجات الجماعية.

#### \* حماية البرمجيات بين تطبيق القانون وأثره على الدول النامية<sup>(١)</sup>:

البرمجيات حسيطة نشاط عالمي متطور أعلي قيم الإبداع وقيم الأفكار والعقل وتعبر عن الاتجاه نحو التحولات الاستراتيجية في مفهوم محددات رأس المال، ومن هنا كانت وسيلة عبور عصر المعلومات بكل إفرازاته، لذا هي مطلوبة للدولة النامية، وأهم موضوعات مشكلة شمال المعلومات

(١) الموقع السابق.

وجنوبها، أنه التجاذب والتضاد بين مالك المعلومة (البرنامج) ومستخدمها، وتقاس في العصر الراهن درجة التقدم بمقدار امتلاك وإنتاج المعرفة، ومن أسف أن الدول النامية مستهلكة لإنتاج الدول المتقدمة المعرفي، مع أن الخوارزميات التي تكتب بها برامج الحاسوب من وضع عالم الرياضيات العربي (الخوارزمي) ومنسوبة لإسمه، وهو ما يضع الدول النامية أمام تحد أكبر أن أرادت تجاوز معيقات نمائها، فالدولة النامية وإن كان وجودها الضعيف لم ينسبته باستهلاك الإنتاج المادي للغرب، فإن وجودها الحقيقي مرهون بإنتاج معارفها الخاصة خشية الذوبان المطلق في معارف الغير، ولعل هذا ما يتعين فهمه من تحديات العولمة، ودون الخوض في إشكالية الموقف منها، ولو ضيقنا مفهومها من حيث البعد التقني إلى القدرة على إنتاج المعرفة التقنية، ونموذجها البرمجيات، فإن معنى هذا أننا بأمس الحاجة لامتلاك أدوات هذه المعرفة، واستلها المميز من معارف الآخرين، إلا لتبرير الاعتداء على حقوق الغير، ولكن ضمن سياسة الحصول على أفضل ميزات من منتجي ما نحتاجه من برامج لهذا الغرض. وقد حققت دولة عربية كمصر والإمارات شروطا تفاوضية إيجابية مع اتحاد منتجي البرمجيات والشركات الدولية الكبرى، تركزت حول إجازة استخدام البرمجيات ببدلات رمزية أو مخفضة من قيمة بدلاتها التسويقية مع حلول المنتجات الموجودة في السوق وصلت حد سحب غير المرخص منها وتزويد نسخ مطورة كبديل عنها، والاتفاق على ما سمي باتفاقات الاستخدام التعليمية أو الإنتاجية أو غيرها، وبكل الحالات فإن المنتج الأجنبي مستفيد أيا كانت تنازلاته، لأن قبوله التعاون بشروط لصالح الدولة النامية سيحقق له ضمانا لتطوير أنشطته القرصنة وإنهاء أسواقها السوداء وسيساهم في خلق قبول جماعي للتعاطي مع متطلبات نظام الملكية الفكرية.

أن التفاوض مع المنتج الأجنبي مترافقا مع تنظيم السوق إراديا وضمن سياسات التعاون علي تخفيف الآثار المتوقعة لإنفاذ نظام الحماية، ومراعاة احتياجات الدول النامية المعرفية وظروفها الاقتصادية وحاجاتها نحو الاتجاه إلسي صناعة البرمجيات وتطويرها وإثرائها، كل تلك روافع أساسية لتطبيق القانون، دون أن نتناسي أن الحديث عن القرصنة يجب أن يوضع في إطاره الموضوعي والواقعي دون مبالغة.

أن نماء استخدام الإنترنت يضع أصحاب الحقوق علي البرمجيات في تحد هائل، وتطور أسواق القرصنة عالميا عبر الشبكة وعبر وسائل لا تطالها القانون في كثير من الأحيان يجعلها مدركة لطلبات الدول النامية المشروعة سيما وأن استخدام التقنية حصيلة لسياسات ضخ المنتجات للاستهلاك في الدول النامية، وهي سياسات لم تخترها هذه الدول وإنما أرادتها الشركات المنتجة، لذا ليس صعبا أن نسمع متطلبات الإنفاذ السلس والصحيح لنظم الحماية لمنتجاتها، وما نقوله في هذا المقام ليس مطالبات أو منح إنما التزام قرره الاتفاقيات الدولية ذات العلاقة، وإلا ما تفسيرنا لمبدأ الدولة الأولى بالرعاية ومبدأ منع الاحتكار ورفض السياسات الإغراقية، ومبادئ حماية المنتج الوطني، ومبادئ حظر قيود الملكية الفكرية كلما كانت ذات أثر سلبي علي إثماء حركة التجارة، وغيرها الكثير من المبادئ التي أقرتها اتفاقيات التجارة الدولية وغيرها، فإذا كان إنفاذ هذه الاتفاقيات يوجب تنفيذ الدولة النامية لالتزاماتها فإن ما طالبت به الدول النامية في ملتقيات التفاوض الدولية إنما هو التفعيل المتوازي لهذه المبادئ عند إنفاذ وتفعيل قواعد ومتطلبات الالتزام<sup>(١)</sup>.

إننا في العالم العربي نتجه نحو سياسات طموحة وهامة في حقل تقنية المعلومات وصناعة البرمجيات، وهذا يطرح تحديات كبرى أمامنا لا نقل عن

---

(١) لموقع سبق.

تحدي تهيئة فرض الاستثمار، ولعل ما نري أهميته الأولى - بعيداً عن التعارض في الموقف من نظام الحماية- تنظيم سوق البرمجيات والخدمات التقنية، لأن مثل هذا التنظيم يتيح اعتماد المعايير والمواصفات وبتنظيم إشاعة قواعد مهنية تحدد السلوك التجاري وبتنظيم سهولة تحقيق القطاع لمتطلباته في التفاوض مع الجهات الدولية والإقليمية، ومن هنا ندعو إلى وقفة أكثر جده لجهة تنظيم القطاع وتحديد متطلبات نموه وتطوير أدائه، فالتنظيم رافعة من روافع إنفاذ القانون بشكل إرادي مقبول للكافة وفوق ذلك أهم روافع إنجاز مكاسب جماعية للوطن كله في العلاقة مع الأطراف الأخرى. وهو الوسيلة لحل مشكلات القطاع بين مالكي الحقوق ومستخدمي المنتجات والعاملين في تسويقها.

### ٣- الاتجاه التشريعي للاعتراف بالحماية القانونية للمصنفات الرقمية<sup>(١)</sup>:

أن حماية البرمجيات وقواعد البيانات وطبوغرافيا الدوائر المتكاملة، كان واحداً من اهتمامات المؤسسات التشريعية في العديد من الدول منذ الثمانينات (وبعضها قبل ذلك)، وتعد موجه التشريع في حقل حماية هذه المصنفات الموجهة الثالثة لتشريعات عصر المعلومات أو ما يطلق عليه قانون الكمبيوتر سبقتها- كما أوضحنا في الفصل الأول- تشريعات حماية البيانات الخاصة (الخصوصية) وتشريعات جرائم الكمبيوتر.

وقد خضعت تشريعات الملكية الفكرية في هذا الحقل إلى العديد من التعديلات الناجمة عن ضرورة التقاطع والتواء مع الطبيعة المتغيرة والسريعة لحقائق وابتكارات عصر المعلومات، الذي كانت سمته التحولات الدراماتيكية في زمن قياسي.

---

(١) الموقع السابق.

أن الوقوف التفصيلي علي محتوى هذه التشريعات واتجاهات الحماية وقواعدها سيكون موضع الكتاب الثالث من هذه الموسوعة، ونكتفي في هذا المقام بإبرام ما أظهره البحث التحليلي بشأن السمات العامة لهذه التشريعات، وتعداد قائمة القوانين الوطنية التي تناولت بالمعالجة والتنظيم الحماية القانونية لمصنفات المعلوماتية المذكورة، وتسهيلا للعرض فإننا نظمنا جداول تحدد السمات العامة والمحتوي العام لتشريعات حماية البرمجيات وقواعد البيانات والدوائر المتكاملة وقائمة بهذه التشريعات علي نحو ما انتهجنا بالنسبة لبقية موضوعات قانون الكمبيوتر. أما بالنسبة للنشر الإلكتروني وأسماء المواقع فكما قدمنا فإن الجهود التشريعية لما نزل في مرحلة المخاض حتى بالنسبة للدول التي قطعت شوطا في التدابير التشريعية في هذا الحقل، إذ لما نزل عناصر هاتين المسألتين محل جدل واسع تلقى بظلالها علي محتوى التشريع وقواعد التنظيم<sup>(1)</sup>.

تشريعات حماية الملكية الفكرية ( Protection of Intellectual Property) في حقل (البرمجيات - Computer programs، وقواعد المعلومات Databases، والدوائر الطبوغرافية - topographies).

خصائص ومحتوي تشريعات حماية الملكية الفكرية المتصلة بتقنية المعلومات.

قوانين حق المؤلف/ الملكية الفكرية (Copyright laws) مسماها الشائع تشريعات حماية حقوق المؤلف المادية والمعنوية علي إنتاجه من البرمجيات وقواعد المعلومات ودوائر الطبوغرافيا (الدوائر المتكاملة)، إضافة إلي الاتجاه الحديث لحماية أسماء النطاقات ومحتوى المواقع علي الإنترنت والمواد محل التجارة الإلكترونية. وصفها العام.

---

(1) الموقع السابق.



سنت هذه التشريعات لتوفير الحماية القانونية للمصنفات المتصلة بالتقنية العالمية الموضوعة من قبل مؤلفيها ضمن جهدهم الفكري، وبعد حسم الجدل حول نظام الحماية من حيث إخضاعها (وتحديدًا البرامج وقواعد البيانات) للحماية الفكرية (الأدبية والفنية وليس الملكية الصناعية (براءات الاختراع) مع مراعاة أن المنتجات التقنية الصناعية كأجهزة أو نحوها التي تصلح للاستغلال الصناعي تعد من قبيل براءات الاختراع إضافة إلى أن حماية الدوائر المتكاملة يقع ضمن نطاق خاص لما ينطوي عليه من عناصر تتصل بحماية الملكية الأدبية وحماية الملكية الصناعية. وقد تزايد الاتجاه نحو هذه التشريعات بسبب الاتفاقيات الدولية وتحديدًا اتفاقية تريبس العالمية (واحدة من اتفاقيات منظمة التجارة الدولية) وبسبب اتفاقية واشنطن للدوائر المتكاملة، وبسبب اعتبار برامج الحاسوب من بين مصنفات اتفاقية برن للملكية الأدبية والفنية بموجب الإضافة التي نصت عليها اتفاقية تريبس المذكورة<sup>(١)</sup>.

وتخضع هذه التشريعات للتطوير وإعادة البحث بسبب ما ظهرت من تحديات في ظل النشر الإلكتروني وحماية مواقع المعلومات على الإنترنت. مبرر وجودها.

توفير الحماية القانونية للحق في الإبداع في حق مصنفات التقنية العالية والحق في الاستغلال العادي والمشروع لعائدات هذه المصنفات وذلك ضمن تنظيم وقواعد إدارية ومدنية وجزائية. هدفها ونطاقها.

ثالث موجة تشريعية انطلقت بوجه عام في الثمانينات مع أن بعض الدول اهتمت بموضوعها قبل ذلك (الفلبين تحديدًا)، لكن انطلاقها الفعلي تم في الثمانينات بعد حسم الجدل حول محل الحماية، أي تشريعات حق المؤلف أم براءات الاختراع. وخضعت لتعديلات متتالية وإلى تنظيم خلال الثمانينات

---

(1) لمرجع السابق.

والتسعينات. ولا تزال تخضع للتطوير والتعديل بسبب استحقاقات الاتفاقات الدولية. الحقبة الزمنية لانطلاقها وترتيبها قانون الملكية الفكرية في النظم التي تقر بوجوده استقلالا، أما في النظم التي لا تسلك هذا المسلك فتتوزع قواعده بين القانون المدني، والقانون الجنائي (المسؤولية الجزائية عن الاعتداء على الحقوق المعنوية والمالية للمؤلف بالنسخ غير المشروع وإعادة الإنتاج والنقل)، القانون الإداري (التنظيم الإداري للجهات المناطة بها حماية حقوق المؤلف/ وزارات الثقافة والصناعة والتجارة والإعلام- مكاتب الحماية والمكتبات الوطنية). الفرع القانوني ذو العلاقة.

البرمجيات التشغيلية والتطبيقية الموجودة على أقراص ووسائط التخزين المستقلة أو المخزنة داخل النظم والشبكات إضافة إلى قواعد المعلومات التي تمثل تنظيمًا وتبويبًا لمعلومات ضمن إطار تشغيل وتطبيق برمجي يميزها عن غيرها، والدوائر التقنية المتكاملة ذات البرمجة من مصدرها (جهة الصنع) محلّة ذو العلاقة بالتكنولوجيا.

القواعد القانونية المنظمة للحقوق المعنوية والمالية لمؤلف المصنفات التقنية محل الحماية، وقواعد المنظمة ومدة الحماية والاستثناءات عليها وقواعد التنظيم الإداري لجهات الضبط والحماية الحكومية، وقواعد المسؤولية المدنية والجزائية المتعلقة بالمخالفين بحقوق المؤلف والجزاءات المقررة ونطاق صلاحيات القضاء وإجراءات التحفظية والعقابية والتكميلية وتدابيره الاحترازية. محتواها بوجه عام.

قائمة تشريعات الملكية الفكرية في حقّ التقنية لمختلف دول العالم.<sup>(١)</sup>  
التشريعات وتاريخ سنّها وإعادة سنّها وتعديلاتها الدولة سنة الأساس  
المرسوم الرئاسي رقم ٤٩ تاريخ ١٤/١١/١٩٧٢.

(١) لمرجع سابق.

The Presidential Decree No. 49 of 14 November 1972.

الفلبين 1972 Philippine

١- قانون حق المؤلف لبرامج الحاسوب لسنة ١٩٨٠ المعدل لقانون حق

المؤلف لسنة ١٩٧٤. (حماية البرمجيات).

1- The Computer Software Compyright Act 1980 amending the Compyright Act 1974 (17 U.S.C. 99 101, 117.

٢- قانون القرصنة والتقليد المعدل لعام ١٩٨٢، وقانون حق المؤلف

المعدل لسنة ١٩٨٠. (حماية قواعد المعلومات).

The Piracy and Counterfeiting Amendment Act of 24 May 1982 (17 U.S.C. §506) and the Compyright Act as amended 1980 (17 U.S.C 502).

٣- قانون حماية شرائح اشتباه الموصلات لعام ١٩٨٤. (١)

The Semiconductor Chip Protection Act of 8 November 1984

الولايات المتحدة الأمريكية

USA 1980

١- القانون رقم ٤٠٦/٢٩/٧/١٩٨١، المتعلق بالإجراءات العاجلة ضد

النسخ غير المشروع وإعادة الإنتاج (برمجيات وقواعد البيانات)

Law No. 406 of 29 July 1981 Concerning Urgent Measures Against the Unlawful Copying, Reproduction.

٢- النصوص المتعلقة بحماية تصميم أشباه الموصلات لسنة ١٩٨٧.

The Provisions Protecting Semiconductor Product Design of 1987

إيطاليا

Italy 1981

---

(1) المرجع السابق.

١- القانون رقم ٢٨٤ لسنة ١٩٨٢- قواعد معلومات

Law No. 284 of 19 May 1982.

٢- قانون حماية تصاميم دوائر أشباه الموصلات رقم ١٤٢٥ لسنة

١٩٨٦.

The Act on the Protection of the Layout- Design of the Circuitry in Semiconductor Products, Law No. 1425 of 18 December 1986.

٣- قانون حق المؤلف المعدل لسنة ١٩٨٩- برمجيات

The Copyright Amendment Act of 1989 1 July 1989 Sweden 1982.

١- القانون المعدل لقانون حق المؤلف للأعوام ٨٢ و ٨٣ و ٨٨- قواعد

المعلومات.

The Copyright Act 1956 (Amendment) Act 1982 of 13 June 1982, The Copyright Amendment Act 1983, and the Copyright, Designs and Patents Act 1988 (which by section 107 extends liability to a person who "knows or had reason to believe that the article in question is an infringing copy of a Copyright work).

٢- قانون حق المؤلف علي البرمجيات المعدل لسنة ١٩٨٦.

The Copyright (Computer software) Amendment Act 1986.

٣- نظام حماية إنتاج شبه الموصلات لسنة ١٩٨٤<sup>(١)</sup>.

The Semiconductor Product- Protection of Topography- Regulation 1987. بريطانيا

United Kingdom

مرسوم وزارة الثقافة رقم ١٥ لسنة ١٩٨٣- البرمجيات

---

(1) لمرجع سابق.

Decree No.15 of the Minister of Culture of 12 July 1983 .

هنجاريا 1983 Hungary

القانون المعدل لقانون حق المؤلف لسنة ١٩٨٤ المتعلق بالمعلوماتية -  
البرمجيات. .

The Copyright Amendment Act 1984 on Informatics

استراليا 1984 Australia

القانون المعدل لقانون حق المؤلف لسنة ١٩٨٤ - برمجيات. (١)

The copyright Amendment Act No. XIX of 1984.

الهند India:

القانون المعدل لقانون حق المؤلف رقم ١١٤ لسنة ١٩٨٤ - البرمجيات.

The Copyright Amendment Act No. 114 of 8 October 1984.

المكسيك Mexico:

١- قوانين حق المؤلف المعدلة لقانون الأعمال الأدبية والفنية لسنة  
١٩٨٤ ذوات الأرقام ٣٤ لعام ٩١ و٤١٨ لعام ٩٣ و٤٤٦ لعام ١٩٩٥  
البرمجيات وقواعد المعلومات.

The copyright Amendment Acts No. 34/1991 of 11 January 1991, No. 418/1993 of 7 May 1993 and No. 446/1995 of 24 March 1995 the Act Amending the Act Relating to copyright in Literary and Artistic works (law No.442) of 8 June 1984.

٢- قانون حماية طوبوغرافية اشباه الموصلات رقم ٣٢ لسنة ٩١

The Act on the protection of Semiconductor Topographies No.32/1991 of 11 January 1991.

---

(1) المرجع السابق.

: فنلندا Finland

قانون الملكية الفكرية لعام ٨٥ - برمجيات.<sup>(١)</sup>

The law on Intellectual property of 7 October 1985.

:تشيلي Chile 1985

١- القانون المعدل لقانون حق المؤلف لعام ٨٥ والمعدل مرة أخرى عام ٩٣ - برمجيات.

The Copyright Amendment Act of 24 June 1985 and further amendments in second Act to Amend the copyright Act of 9 June 1993.

٢- قانون حماية طبوغرافية الشرائح الإلكترونية لأشباه الموصلات لعام ٨٧ المعدل عام ٩٠.

The act on the protection of topographies of Mico-Electronic Semiconductor products of 22 October 1987 as amended 1990.

٣- المادة السابعة من قانون خدمات المعلومات والاتصالات لعام ١٩٩٧.

Article 7 information and communication services Act of 22 July 1997.

:ألمانيا Germany

١- القانون رقم ٦٦٠ لعام ١٩٨٥ - برمجيات.

Law No. 85 660 of 3 July 1985.

٣- قانون حماية طبوغرافية منتجات أشباه الموصلات رقم ٨٩٠ لسنة ١٩٨٧.

The act on the protection of the Topographies of Semiconductor products, Law No. 87 890 of 4 November 1987.

---

(1) المرجع السابق.

فرنسا France: (١)

١- قانون المعدل لقانون حق المؤلف لعام ١٩٨٥.

The Copyright Amendment Act of 7 June 1985.

٢- قانون الدوائر المتكاملة واشباه الموصلات لعام ١٩٨٥.

The Act Concerning the circuit Layout of a Semiconductor Integrated circuit of 31 May 1985.

اليابان Japan:

قانون حق المؤلف لعام ١٩٨٥.

The Copyright Law of 1985.

تايوان / China :Taiwn / China

القانون رقم ٦٤٦ لسنة ١٩٨٧.

Law No. 7.646 of 18 December 1987.

البرازيل Brazil 1987:

١- القسم ٤٢ من قانون حق المؤلف المعدل لسنة ١٩٨٧ - قواعد معلومات.

Section 42 copyright act as amended in 1987.

٢- قانون حق المؤلف المعدل لعام ١٩٨٨ - برمجيات.

The Copyright Amendment act 1988.

قانون دوائر الطبوغرافية المتكاملة لعام ١٩٩٠.

The Integrated circuit topography act ( S.C. 1990).

كندا Canada:

١- قانون رقم ٢٢ لسنة ٨٧ المتعلق بالملكية الفكرية وفق آخر تعديل لعام

١٩٩٦. (٢)

---

(1) المرجع السابق.

(2) المرجع السابق.

Law No. 22/1987 on Intellectual property of 11 November 1987, latest version passed by R.D.1 / 1996 on 12 April 1996.

٢- قانون الحماية القانونية لطوبوغرافية اشباه الموصلات لعام ١٩٨٨.

Law on the legal protection of the Topographies of Semiconductor products of 3 May 1988.

٣- المادة ٢٠٧ من القانون الجنائي لعام ١٩٩٥.

Articles 207 et seq. Criminal code 1995.

اسبانيا Spain:

١- قانون ١٩٨٧ لحماية الطوبوغرافيا الأصلية لمنتجات اشباه الموصلات.

The act of 24 October 1987 on the protection of original Topographies of semiconductor products.

٢- قانون حق المؤلف لعام ١٩٩٤ - برمجيات وقواعد معلومات.

Copyright act of 7 July 1994.

هولندا Netherlands:

١- قانون حماية إنتاج اشباه الموصلات رقم ٧٧٨ لسنة ١٩٨٧.

The act on the protection of Semiconductor products, law No. 778 of 9 December 1987.

٢- القانون رقم ١٥٣ لسنة ١٩٨٨.

Law No. 153 of 14 January 1988.

الدنمارك Denmark:

أمر / تعليمات حق المؤلف رقم ١٩١١ كما عدلت عام ١٩٨٨.

The copyright Ordinance 1911 as amended in 1988.

اسرائيل Israel 1988:

١- قانون حماية اشباه الموصلات رقم ٣٧٢ لسنة ١٩٨٨.

The Semiconductor Protection Act ( 1988/372).



٢- قانون حق المؤلف رقم ٩٣ لسنة ١٩٩٣ المعدل رقم ١٥١ لسنة ١٩٩٦.

(برمجيات وقواعد معلومات):

Copyright Amendment act 1993 /93 as amended in 151/1996.

النمسا Austria: (١)

قانون حق المؤلف المعدل لعام ١٩٩٠.

The copyright Amendment act of 15 June 1990.

النرويج Norway 1990:

١- القانون رقم ٢٢ لسنة ١٩٩٢ قانون حماية حق المؤلف المعدل بالقانون ١٤ لسنة ١٩٩٨ و٢٩ لسنة ١٩٩٩. ويشمل حماية البرمجيات وقواعد البيانات.

٢- قانون حماية التصميمات للدوائر المتكاملة رقم ١٠ لسنة ٢٠٠٠.

الأردن Jordan 1992:

القانون الاتحادي رقم ٤٠ لسنة ١٩٩٢ ولائحته التنفيذية ويتضمن حماية برامج الحاسوب. الإمارات العربية المتحدة

القانون رقم ١٠ لسنة ١٩٩٣ - برامج الحاسوب محل حماية البحرين ١٩٩٣  
قانون ٢٩ لسنة ١٩٩٤ المعدل لقانون ١٩٥٤ وتضمن حماية برامج الحاسوب وقواعد البيانات . مصر ١٩٩٤.

القانون ٣٦ لسنة ١٩٩٤ - تونس

قانون ٢٥ لسنة ١٩٩٥ - حماية برامج الحاسوب قطر ١٩٩٥.

قانون ١٩٩٥ المعدل لقانون حق المؤلف لعام ١٩٧٢.

The act of 24 April 1995 amending the copyright act of 29 march 1972.

---

(1) المرجع السابق.

لوكسمبورغ 1995 Luxembourg: (١)

قانون ٤٧ لسنة ١٩٩٦ عمان ١٩٩٦.

قانون ١٠ لسنة ١٩٩٧ الجزائر ١٩٩٧.

قانون ٧٥ لسنة ١٩٩٩ ( برامج وقواعد بيانات ) لبنان ١٩٩٩ المرسوم  
بقانون رقم ٥ لسنة ١٩٩٩، البرامج وقواعد البيانات الكويت.

٣- قواعد واشكالات حماية مصنفات المعلوماتية:

شهدت المنطقة العربية مؤخرا جملة من دعاوى الملكية الفكرية بخصوص  
برامج الحاسوب والتسجيلات الصوتية إضافة إلى عدد من المناعات في  
ميدان الألعاب الإلكترونية بمختلف أنواعها، ويعزى النشاط المتزايد في هذا  
الميدان إلى ما تقرر من تفعيل تطبيق قوانين حق المؤلف وإلى نشاط  
الشركات الأجنبية المترافق مع سياسات تحرير التجارة في السلع.

#### خصوصية جرائم الكمبيوتر والانترنت: (٢)

إن ظاهرة جرائم الحاسب الآلي، ظاهرة إجرامية جديدة مستحدثة تفرع  
في جنباتها أجراس الخطر لتتبع مجتمعات العصر الراهن لحجم المخاطر  
وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الاعتداء على  
المعطيات بدلالاتها التقنية الواسعة ( بيانات ومعلومات وبرامج بكافة أنواعها).  
إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات.

إن ظاهرة جرائم الحاسب الآلي، ظاهرة إجرامية جديدة مستحدثة تفرع  
في جنباتها أجراس الخطر لتتبع مجتمعات العصر الراهن لحجم المخاطر

(1) المرجع لسابق.

(2) <http://www.barasy.com/index.php?Name=pages&op=page&pid=110>

- النادي العربي للمعلوماتية.

وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الاعتداء على المعطيات بدلائنها التقنية الواسعة ( بيانات ومعلومات وبرامج بكافة أنواعها).  
فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أنكباء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات<sup>(١)</sup>.

وتتبع أهمية هذا الموضوع من دور الثورة المعلوماتية في عملية التنمية الشاملة بنوعها الاقتصادي والاجتماعي وحاجتها من ثم إلى بحث المشكلات القانونية المتعلقة بها ومحاولة الوصول إلى إيجاد الحلول المناسبة لها.  
ومن ناحية أخرى، فإن المعلوماتية باعتبارها ظاهرة إنسانية واقتصادية واجتماعية لا يمكن أن تتطور بذاتها دون أن تتوافر لها القواعد القانونية التي تنظم استغلالها.

وأصبح الحاسب الآلي على مدى الفترة الماضية ركيزة أساسية لأهداف التطور في شتى مناحي الحياة، سواء تمثلت في أنشطة اقتصادية أو علمية أو صناعية أو زراعية<sup>(٢)</sup>.

وترتب على الاستخدام المتزايد لنظم المعلومات سواء في شكل أموال معلوماتية " biens Informatiques " أو أساليب مستحدثة إلى نشوء ما يعرف بالجريمة المعلوماتية، وهي نتيجة حتمية لكل تطور علمي أو تقني مستحدث، ويرتكن هذا النوع من الاجرام على محورين أولهما ضد المال والثاني ضد الأشخاص ويستمد نشاطه من القدرات الهائلة من الحاسب الآلي.

---

(١) النادي العربي للمعلوماتية  
(٢) الموقع السابق.

ويرى الأستاذ Parker أن الجريمة المعلوماتية ( كل فعل إجرامي أو متعمد أيا كانت صلته كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق -المجني عليه، أو كسبا يحققه الفاعل).

بينما يرى خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية أن المفصود بالجريمة المعلوماتية هي ( كل سلوك غير مشروع أو مناف لأخلاق أو غير مسموح به، يرتبط بالمعالجة الآلية للبيانات أو بنقلها).

ويجمع الفقه الفرنسي بصفة عامة على القول بأن فكرة الغش المعلوماتي Fraude Informatique التي تعادل جريمة الكمبيوتر computer related crim anglo saxon وهي تشمل العديد من عدة أفعال متنوعة وليس المقصود بها وصفا ولكنها بالأخرى ينظر إلى هذا المصطلح بوصفه مصطلحا خاصا بعلم الاجرام، وهذا المصطلح يكتنفه غموض على قدر كبير وربما يكون له معان متعددة لكي يمكن أن نحدد مجموعة قانونية مباشرة تطبق على مستوى القانون الجنائي.

وتتميز أفعال الجريمة المعلوماتية على نحو قليل في مضمونها وتنفيذها أو محو آثارها عن تلك الخاصة بالجريمة التقليدية حيث يكفي للمجرم المعلوماتي أن يلمس لوحة مفاتيح الحاسب الآلي والتي تقوم على الفوز بعمليات الحساب والتحليل وإسقاط الحواجز وأساليب الحماية الأكثر خداعا. وأيضا تتميز جرائم الحاسب بالصعوبات البالغة في اكتشافها وبالعجز في حالات كثيرة عن إمكان إثباتها في حالة اكتشافها.

**ومرد ذلك الأسباب التالية<sup>(١)</sup>:**

**أولا:** لا تخلف جرائم الحاسب آثارا ظاهرة خارجية فهي تنصب على البيانات والمعلومات المخزنة في نظم المعلومات والبرامج مما ينفي وجود

(١) النادي العربي للمعلوماتية.

أى أثر مادي يمكن الاستعانة به في إثباتها، فالجرائم المعلوماتية ينتفي فيها العنف وسفك الدماء ولا توجد فيها آثار لاقتحام سرقة الأموال، وإنما هي أرقام ودلالات تتغير أو تمحى من السجلات ومما يزيد من هذه الصعوبة ارتكابها في الخفاء، وعدم وجود أثر كتابي مما يجرى من خلال تنفيذها من عمليات حيث يتم نقل المعلومات بواسطة النبضات الإلكترونية.

ثانياً: يستم ارتكاب جريمة الحاسب عادة عن بعد فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها<sup>(1)</sup>.

ثالثاً: وتبدو أكثر المشكلات جساماً لا في مجال صعوبة اكتشاف وإثبات جرائم الحاسب بل وفي دراسة هذه الظاهرة في مجملها هي مشكلة امتناع المجنسي عليهم عن التبليغ عن الجرائم المرتكبة ضد نظام الحاسب وهو ما يعرف بالرقم الأسود Chiffrenoir حيث لا يعلم ضحايا هذه الجرائم شيئاً عنها إلا عندما تكون أنظمتهم المعلوماتية هدفاً لفعل الغش أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل.

ويلزم للمجتمع المعلوماتي في مجال قانون الإجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق في مجال جرائم الكمبيوتر.

والسبب في ذلك أن محترفي انتهاك شبكات الحاسب الآلية ومرتكبي الجرائم الاقتصادية وتجار الأسلحة والمواد المخدرة يقومون بتخزين معلوماتهم في أنظمة تقنية المعلومات وعلى نحو متطور، وتصطلم الأجهزة

---

(1) الموقع السابق.

المكلفة بالتحقيق بهذا التكتيك لتخزين المعلومات وهي التي تسعى للحصول على أدلة الإثبات<sup>(١)</sup>.

وتصادف الصعوبات عندما يتعلق الأمر على وجه الخصوص بتخزين بيانات بالخارج بواسطة شبكة الاتصالات البعيدة Telecommunication ويصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن نحدد إلى أى مدى تكفى الأساليب التقليدية للإكراه فى قانون الإجراءات الجنائية من أجل مباشرة تحقيقات ناجحة فى مجال تقنية المعلومات. وقد اقترن بظهور تقنية المعلومات مشكلات خاصة ومستحدثة وعلى سبيل المثال التفتيش والتخفظ على المعلومات وإلزام الشاهد باسترجاع وكتابة المعلومات والحق فى مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الاتصالات البعيدة وجمعها وتخزينها وضم المعلومات الأسمية إلى الدعوى الجنائية. وأهم ما يميز جرائم نظم المعلومات صعوبة اكتشافها وإثباتها وهى صعوبة يعترف بها جميع الباحثين فى هذا المجال علاوة على ما تتميز به إجراءات جمع الأدلة فى هذا المجال من ذاتية خاصة<sup>(٢)</sup>.

ومجموعة الأعمال التى يرى المحقق وجوب أو ملاءمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة يهتم بها قانون العقوبات هى إجراءات التحقيق. وتنقسم هذه الإجراءات إلى قسمين: قسم يهدف إلى الحصول على الدليل كالتفتيش وسماع الشهود وقسم يمهد للدليل ويؤدى إليه كالقبض والحبس الاحتياطي. وتسمى المجموعة الأولى: إجراءات جمع الأدلة أما الثانية: فتعرف بالإجراءات الاحتياطية ضد المتهم. وسوف يقتصر بحثنا هذا على الإجراءات الخاصة بجمع الأدلة وهذه الإجراءات تنطوى أيضا على المساس بالحريات وهذا أبرز ما يميزها ولهذا فإنه يجب النظر إليها باعتبارها واردة

(١) النادي العربي للمعلوماتية.

(٢) الموقع لسابق.

على سبيل الحصر فلا يجوز للمحقق أن يباشر إجراء آخر فيه مساس بحريات الأفراد ولو كان من شأنه أن يؤدي إلى كشف الحقيقة كاستعمال جهاز كشف الكذب أو مصل الحقيقة.

وإجراءات جمع الأدلة كما حددها القانون هي:

المعاينة، ندب الخبراء، التفتيش، ضبط الأشياء، ومراقبة المحادثات وتسجيلها وسماع الشهود والاستجواب والمواجهة. وليس على المحقق الالتزام بإتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساسا لمباشرتها جميعا وإنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقتضي به المصلحة وما تسمح به هذه الظروف وسوف نوضح في مجال جمع الأدلة ما يلي<sup>(1)</sup>:

أولاً: معاينة مسرح الجريمة والمعلوماتية

ثانياً: التفتيش في مجال الجريمة المعلوماتية.

ثالثاً: الشهادة في الجريمة المعلوماتية.

رابعاً: الخبرة في مجال الجريمة المعلوماتية.

خامساً: الضبط في مجال الجريمة المعلوماتية.

أولاً: معاينة مسرح الجريمة المعلوماتية

يقصد بالمعاينة فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، كمعاينة مكان ارتكاب الجريمة أو أداة المعاينة قد تكون إجراء تحقيق لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من مرق أو نقوب. ويلاحظ أن المعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس

---

(1) المرجع السابق. النادي العربي للمعلوماتية.

بحقوق الأفراد، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال وإذا اقتضت دخول مسكن أو له حرمة خاصة كانت إجراء تحقيق.

والمعاينة جوازية للمحقق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم أو لم يطلبوها. ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية.

ومرد ذلك إلى اعتبارين:

١- أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يترتب على ارتكابها آثار مادية<sup>(١)</sup>.

٢- أن عدد كبيراً من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة إرتكاب الجريمة واكتشافها مما يهيئ الفرصة لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي:

- تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته وإبراعي تسجيل وقت وتاريخ ومكان التقاط كل صورة.
- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات

---

(١) للنادي العربي للمعلوماتية  
(٢) المرجع السابق.



المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذى تم عن طريقة الولوج إلى النظام أو الموقع أو الدخول معه فى حوار.

• ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء<sup>(١)(٢)</sup>.

• عدم نقل أى مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أى مجالات لقوى مغناطيسية يمكن أن تتسبب فى محو البيانات المسجلة.

• التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة رغير السليمة أو المحطمة وفحصها ورفع البصمات التى قد تكون لها صلة بالجريمة المرتكبة.

• التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات.

• إعداد خطة للهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على أن تكون الخطة موضحة بالرسومات ويتم مراجعتها مع أعضاء الفريق قبل التحرك مع الأخذ فى الاعتبار قاعدة smeac العسكرية والتى تعنى حالة situation الرسالة mission التنفيذية execution المداخل والمخارج avenues of approach والاتصالات communication وهى ملائمة للأجهزة الأمنية وأجهزة تنفيذ القوانين فالحالة أو الوضع يعنى معرفة حجم القضية التى تقوم بالتحقيق فيها، وعدد المتورطين فيه أما الرسالة فهى

---

(1) الموقع السابق.  
(2) النادي العربى للمعلوماتية.

تحدد الهدف من الغارة والتنفيذ يعني كيفية أداء المهمة أما المداخل والمخارج فإن معرفتها ضرورية وهي تختلف من جريمة لأخرى وتحسب وفقا لمكونات طريق التحقيق بينما يأتي عنصر الاتصالات لضمان السرية وسلامة التعامل وتبادل المعلومات أثناء مهمة الغارة.

وبعد وصول الفريق إلى مسرح الجريمة أو مكان الغارة يتم التأمين والسيطرة على المكان والبدء في التفتيش على النحو التالي<sup>(1)</sup>:

أ- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان الإغارة وذلك عن طريق إغلاق الطرق والمداخل.

ب- السيطرة على الدائرة المحيطة بمكان الإغارة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة ورصد الاتصالات الهاتفية من وإلى مكان الإغارة مع إبطال أجهزة الهاتف النقال.

ج- تأمين موقع الغارة والسيطرة على جميع أركانها ومداخلها والتحكم على الأشخاص الموجودين.

د- تحديد أجهزة الحاسب الآلي الموجودة في مكان الإغارة وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكات اتصالات يجب البحث عن خادم الملف file server لتعطيل حركة الاتصالات.

هـ- يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات من على البعد أو من جهاز آخر داخل المبنى.

و- اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيدا عن أجهزة الحاسب الآلي.

---

(1) النادي العربي للمعلوماتية.

## ثانيا: التفتيش فى مجال الجريمة المعلوماتية<sup>(١)</sup>

التفتيش فى قانون الإجراءات هو البحث عن شئ يتصل بجريمة وقعت ويفيد فى كشف الحقيقة عنها وعن مرتكبها وقد يقتضى التفتيش إجراء البحث فى محل له حرمة خاصة وقد أحاط القانون هذا التفتيش بضمانات عديدة ومحل التفتيش إما أن يكون مسكنا أو شخصا، وهو بنوعيه قد يكون متعلقا بالمتهم أو بغيره وهو فى كل أحواله جائز مع اختلاف فى بعض الشروط.

وسوف نقسم الدراسة إلى:

١- مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش.

٢- ضوابط تفتيش نظم الحاسب الآلي.

١- مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش:

يتكون الحاسب الآلي من مكونات مادية Hard Ware مكونات منطقية Soft ware كما أن له شبكات اتصالات بعدية سلكية ولا سلكية سواء على المستوى المحلى أو المستوى الدولى فهل تخضع هذه المكونات للتفتيش؟

أ- مدى خضوع مكونات الحاسب المادية للتفتيش:

يخضع الولوج فى المكونات المادية للحاسب بحثا عن شئ يتصل بجريمة معلوماتية وقعت ويفيد فى كشف الحقيقة عنها وعن مرتكبها للإجراءات القانونية الخاصة بالتفتيش وبعبارة أخرى فإن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو مكان عام أم مكان خاص إذ أن لصفة المكان أهمية خاصة فى مجال التفتيش فإذا كانت موجودة فى مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا فى الحالات التى يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونيا فى التشريعات المختلفة.

(١) المرجع السابق.

ويجب التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصلة بحاسب أو بنهاية طرفية terminal في مكان آخر كمسكن لا يخص مسكن المتهم فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة، تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية أو كان مسيطراً عليها أو حائزاً لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال.

#### ب- مدى خضوع مكونات الحاسب المعنوية للتفتيش: (١)

بالنسبة لتفتيش مكونات الحاسب المعنوية فقد ثار الخلاف بشأن جواز تفتيشها حيث يذهب رأى أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها.

وفى هذا المعنى نجد المادة ٢٥١ من قانون الإجراءات الجنائية اليوناني تعطي سلطات التحقيق إمكانية القيام (بأى شئ يكون ضروريا لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة أى شئ بأنها تشمل بالضبط البيانات المخزنة أو المعالجة إلكترونياً، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في اليونان إذ بمقتور المحقق أن يعطي أمراً للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية.

وتمنح المادة ٤٨٧ من القانون الجنائي الكندي سلطة إصدار إذن لضبط أى شئ طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه في

---

(١) الموقع السابق.

ارتكابها أو أن هناك نية في أن يستخدم في ارتكاب الجريمة، ينتج دليلاً على وقوع الجريمة.

#### إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات: (١)

إن ظاهرة جرائم الحاسب الآلي، ظاهرة إجرامية جديدة مستحدثة تفرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الإعتداء على المعطيات بدلائلها التقنية الواسعة (بيانات ومعلومات وبرامج بكافة أنواعها). فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أنكسياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

وتتبع أهمية هذا الموضوع من دور الثورة المعلوماتية في عملية التنمية الشاملة بنوعيتها الاقتصادية والاجتماعي وحاجتها من ثم إلى بحث المشكلات القانونية المتعلقة بها ومحاولة الوصول إلى إيجاد الحلول المناسبة لها. ومن ناحية أخرى، فإن المعلوماتية باعتبارها ظاهرة إنسانية واقتصادية واجتماعية لا يمكن أن تتطور بذاتها دون أن تتوافر لها القواعد القانونية التي تنظم استغلالها.

وأصبح الحاسب الآلي على مدة الفترة الماضية ركيزة أساسية لأهداف التطور في شتى مناحي الحياة، سواء تمثلت في أنشطة اقتصادية أو علمية أو صناعية أو زراعية<sup>(٢)</sup>.

(1) <http://www.barasy.com/index.php?Name=pages&op=page&pid=110>

الرائد أ/ الدكتور/ هبة الله حسين علي محمود.  
(2) المرجع السابق.

وترتب على الاستخدام المتزايد لنظم المعلومات سواء فى شكل أموال معلوماتية " biens Informatiques " أو أساليب مستحدثة إلى نشوء ما يعرف بالجريمة المعلوماتية، وهى نتيجة حتمية لكل تطور علمي أو تقني مستحدث، ويرتكب هذا النوع من الأجرام على محورين أولهما ضد المال والثاني ضد الأشخاص ويستمد نشاطه من القدرات الهائلة من الحاسب الآلي. ويرى الأستاذ Parker أن الجريمة المعلوماتية ( كل فعل إجرامي أو مستعند أيضا كانت صلته كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسبا يحققه الفاعل).

بينما يرى خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية أن المقصود بالجريمة المعلوماتية هى ( كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به، يرتبط بالمعالجة الآلية للبيانات أو بنقلها).

ويجمع الفقه الفرنسي بصفة عامة على القول بأن فكرة الغش المعلوماتي Fraude Informatique التى تعادل جريمة الكمبيوتر computer related crim anglo saxon وهى تشمل العديد من عدة أفعال متنوعة وليس المقصود بها وصفا ولكنها بالأخرى ينظر إلى هذا المصطلح بوصفه مصطلحا خاصا بعلم الأجرام، وهذا المصطلح يكتنفه غموض على قدر كبير وربما يكون له معان متعددة لكي يمكن أن نحدد مجموعة قانونية مباشرة تطبق على مستوى القانون الجنائي.

وتتميز أفعال الجريمة المعلوماتية على نحو قليل فى مضمونها وتنفيذها أو محو آثارها عن تلك الخاصة بالجريمة التقليدية حيث يكفى للمجرم المعلوماتي أن يلمس لوحة مفاتيح الحاسب الآلي والتي تقوم على الفوز بعمليات الحساب والتحليل وإسقاط الحواجز وأساليب الحماية الأكثر خداعا.

وأيضاً تتميز جرائم الحاسب بالصعوبات البالغة في اكتشافها وبالعجز في حالات كثيرة عن إمكان إثباتها في حالة اكتشافها.

#### ومرد ذلك الأسباب التالية<sup>(١)</sup>:

أولاً: لا تخلف جرائم الحاسب أثراً ظاهرة خارجية فهي تنصب على البيانات والمعلومات المخترنة في نظم المعلومات والبرامج مما ينفي وجود أى أثر مادي يمكن الاستعانة به في إثباتها، فالجرائم المعلوماتية ينتفي فيها العنف وسفك الدماء ولا توجد فيها آثار لاقتحام سرقة الأموال، وإنما هي أرقام ودلالات تتغير أو تمحى من السجلات ومما يزيد من هذه الصعوبة ارتكابها في الخفاء، وعدم وجود أثر كتابي مما يجرى من خلال تنفيذها من عمليات حيث يتم نقل المعلومات بواسطة النبضات الإلكترونية.

ثانياً: يتم ارتكاب جريمة الحاسب عادة عن بعد فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها.

ثالثاً: وتبدو أكثر المشكلات جسامة لا في مجال صعوبة اكتشاف وإثبات جرائم الحاسب بل وفي دراسة هذه الظاهرة في مجملها هي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة ضد نظام الحاسب وهو ما يعرف بالرقم الأسود Chiffrenoir حيث لا يعلم ضحايا هذه الجرائم شيئاً عنها إلا عندما تكون أنظمتهم المعلوماتية هدفاً لفعل الغش أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل.

---

(١) المرجع والموقع السابق.

ويلزم للمجتمع المعلوماتي في مجال قانون الإجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق في مجال جرائم الكمبيوتر .

والسبب في ذلك أن محترفي انتهاك شبكات الحاسب الآلية ومرتكبي الجرائم الاقتصادية وتجار الأسلحة والمواد المخدرة يقومون بتخزين معلوماتهم في أنظمة تقنية المعلومات وعلى نحو متطور، وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكتيك لتخزين المعلومات وهي التي تسعى للحصول على أدلة الإثبات<sup>(1)</sup>.

وتصادف الصعوبات عندما يتعلق الأمر على وجه الخصوص بتخزين بيانات بالخارج بواسطة شبكة الاتصالات البعيدة Telecommunication ويصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية للإكراه في قانون الإجراءات الجنائية من أجل مباشرة تحقيقات ناجحة في مجال تقنية المعلومات. وقد اقترن بظهور تقنية المعلومات مشكلات خاصة ومستحدثة وعلى سبيل المثال التفتيش والتحفظ على المعلومات وإلزام الشاهد باسترجاع وكتابة المعلومات والحق في مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الاتصالات البعيدة وجمعها وتخزينها وضم المعلومات الأسمية إلى الدعوى الجنائية. وأهم ما يميز جرائم نظم المعلومات صعوبة اكتشافها وإثباتها وهي صعوبة يعترف بها جميع الباحثين في هذا المجال علاوة على ما تتميز به إجراءات جمع الأدلة في هذا المجال من ذاتية خاصة.

ومجموعة الأعمال التي يرى المحقق وجوب أو ملاءمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة يهتم بها قانون العقوبات هي إجراءات التحقيق.

---

(1) الموقع والمرجع السابق.



وتنقسم هذه الإجراءات إلى قسمين: قسم يهدف إلى الحصول على الدليل كالتفتيش وسماع الشهود وقسم يمهد للدليل ويؤدي إليه كالقبض والحبس الاحتياطي. وتسمى المجموعة الأولى: إجراءات جمع الأدلة أما الثانية: فتعرف بالإجراءات الاحتياطية ضد المتهم. وسوف يقتصر بحثنا هذا على الإجراءات الخاصة بجمع الأدلة وهذه الإجراءات تتطوّر أيضا على المساس بالحريات وهذا أبرز ما يميزها ولهذا فإنه يجب النظر إليها باعتبارها واردة على سبيل الحصر فلا يجوز للمحقق أن يباشر إجراء آخر فيه مساس بحريات الأفراد ولو كان من شأنه أن يؤدي إلى كشف الحقيقة كاستعمال جهاز كشف الكذب أو مصل الحقيقة<sup>(١)</sup>.

وإجراءات جمع الأدلة كما حددها القانون هي:

المعاينة، ندب الخبراء، التفتيش، ضبط الأشياء، ومراقبة المحادثات وتسجيلها وسماع الشهود والاستجواب والمواجهة. وليس على المحقق الالتزام بإتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساسا لمباشرتها جميعا وإنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقتضي به المصلحة وما تسمح به هذه الظروف وسوف نوضح في مجال جمع الأدلة ما يلي:

أولا: معاينة مسرح الجريمة والمعلوماتية

ثانيا: التفتيش في مجال الجريمة المعلوماتية.

ثالثا: الشهادة في الجريمة المعلوماتية.

رابعا: الخبرة في مجال الجريمة المعلوماتية.

خامسا: الضبط في مجال الجريمة المعلوماتية.

---

(١) الموقع والمرجع السابق.

## أولاً: معاينة مسرح الجريمة المعلوماتية<sup>(١)</sup>

يقصد بالمعاينة فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، كمعاينة مكان ارتكاب الجريمة أو أداة المعاينة قد تكون إجراء تحقيق لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من مزق أو نقوب.

ويلاحظ أن المعاينة قد تكون إجراء تحقيق أو استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال وإذا اقتضت دخول مسكن أو له حرمة خاصة كانت إجراء تحقيق.

والمعاينة جوازية للمحقق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم أو لم يطلبوها. ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية.

ومرد ذلك إلى اعتبارين:

١- أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يترتب على ارتكابها آثار مادية.

٢- أن عدد كبيراً من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة إرتكاب الجريمة واكتشافها مما يهيئ الفرصة لحدوث تغيير أو اتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي:

(١) الموقع والمرجع السابق.

- \* تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته ويراعي تسجيل وقت وتاريخ ومكان التقاط كل صورة.
- \* العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في حوار. <sup>(١)</sup>
- \* ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء.
- \* عدم نقل أى مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أى مجالات لقوى مغناطيسية يمكن أن تتسبب فى محو البيانات المسجلة.
- \* التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة وغير السليمة أو المحطمة وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.
- \* التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات.
- \* إعداد خطة للهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على أن تكون الخطة موضحة بالرسومات وتتم مراجعتها مع أعضاء الفريق قبل التحرك مع الأخذ فى الاعتبار قاعدة smeac العسكرية والتي

(1) الموقع والمرجع السابق.

تعني حالة situation الرسالة mission التنفيذية execution المداخل والمخارج avenues of approach والاتصالات communication وهي ملائمة للأجهزة الأمنية وأجهزة تنفيذ القوانين فالحالة أو الوضع يعني معرفة حجم القضية التي تقوم بالتحقيق فيها، وعدد المتورطين فيه أما الرسالة فهي تحدد الهدف من الغارة والتنفيذ يعني كيفية أداء المهمة أما المداخل والمخارج فإن معرفتها ضرورية وهي تختلف من جريمة لأخرى وتحسب وفقا لمكونات طريق التحقيق بينما يأتي عنصر الاتصالات لضمان السرية وسلامة التعامل وتبادل المعلومات أثناء عملية الغارة. (١)

وبعد وصول الفريق إلى مسرح الجريمة أو مكان الغارة يتم التأمين والسيطرة على المكان والبدء في التفتيش على النحو التالي:

أ- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان الإغارة وذلك عن طريق إغلاق الطرق والمداخل.

ب- السيطرة على الدائرة المحيطة بمكان الإغارة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة ورصد الاتصالات الهاتفية من وإلى مكان الإغارة مع إبطال أجهزة الهاتف النقال.

ج- تأمين موقع الغارة والسيطرة على جميع أركانها ومنافذها والتحكم على الأشخاص الموجودين.

د- تحديد أجهزة الحاسب الآلي الموجودة في مكان الإغارة وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكات اتصالات يجب البحث عن خادم الملف file server لتعطيل حركة الاتصالات.

هـ- بوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات من على البعد أو من جهاز آخر داخل المبنى.

---

(١) الموقع والمرجع السابق.

و- اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيداً عن أجهزة الحاسب الآلي.

#### ثانياً: التفتيش في مجال الجريمة المعلوماتية<sup>(1)</sup>

التفتيش في قانون الإجراءات هو البحث عن شيء يتصل بجريمه وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة وقد أحاط القانون هذا التفتيش بضمانات عديدة ومحل التفتيش إما أن يكون مسكناً أو شخصاً، وهو بنوعه قد يكون متعلقاً بالمتهم أو بغيره وهو في كل أحواله جائز مع اختلاف في بعض الشروط.

وسوف نقسم الدراسة إلى:

١- مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش.

٢- ضوابط تفتيش نظم الحاسب الآلي.

#### ١- مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش:

يتكون الحاسب الآلي من مكونات مادية Hard Ware مكونات منطقية Soft ware كما أن له شبكات اتصالات بعدية سلكية ولا سلكية سواء على المستوى المحلي أو المستوى الدولي فهل تخضع هذه المكونات للتفتيش؟

##### أ- مدى خضوع مكونات الحاسب المادية للتفتيش:

يخضع الولوج في المكونات المادية للحاسب بحثاً عن شيء يتصل بجريمة معلوماتية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها للإجراءات القانونية الخاصة بالتفتيش وبعبارة أخرى فإن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو مكان عام أم مكان خاص إذ أن لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت موجودة في مكان

---

(1) الموقع والمرجع السابق.

خاص كمسكن المتهم أو أحد متحفظاته كان لها حكمة فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه بنفس الضمانات المقررة قانونيا في التشريعات المختلفة.

ويجب التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصلة بحاسب أو بنهاية طرفية terminal في مكان آخر كمسكن لا يخص مسكن المتهم فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال.

#### ب- مدى خضوع مكونات الحاسب المعنوية للتفتيش:

بالنسبة لتفتيش مكونات الحاسب المعنوية فقد ثار الخلاف بشأن جواز تفتيشها حيث يذهب رأى أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها.

وفى هذا المعنى نجد المادة ٢٥١ من قانون الإجراءات الجنائية اليوناني تعطي سلطات التحقيق إمكانية القيام (بأى شئ يكون ضروريا لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة أى شئ بأنها تشمل بالضبط البيانات المخزنة أو المعالجة إلكترونيا، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في اليونان إذ بمقتور المحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية.

وتمنح المادة ٤٨٧ من القانون الجنائي الكندي سلطة إصدار إذن لضبط أى شئ طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه في ارتكابها أو أن هناك نية في أن يستخدم في ارتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة.

#### التحقيق في جرائم الحاسوب:

##### مكافحة الجرائم المعلوماتية قبل وقوعها: الدور الوقائي<sup>(١)</sup>:

نظرا لطبيعة الجرائم المعلوماتية الخاصة، لا يستطيع عناصر الضابطة العدلية أن يؤدوا دورا إيجابيا في هذا المجال.

إلا أنه بالنظر إلي كون البرامج المعلوماتية تشكل قيما فكرية محمية بموجب القوانين الحديثة، يقتصر دور رجال الضابطة العدلية في الحفاظ علي هذه البرامج من النسخ غير المشروع عبر التأكد من التزام المتعاملين في هذه البرامج بالحصول علي ترخيص من مالكيها للتعامل بها.

ويتسبلور دورها، علي هذا الصعيد، عبر مراقبتها للمحلات التجارية، بواسطة وحدات متخصصة من عناصرها، للحؤول دون وقوع التعدي علي برامج الحاسب الآلي أو لمنع استمراره.

- مكافحة الجرائم المعلوماتية بعد وقوعها: الدور القمعي:

- معاينة مسرح الجرائم المعلوماتية.

لا تواجه رجال الضابطة العدلية أي صعوبة تذكر عند معاينتهم لمسرح الجريمة الواقعة علي المكونات المادية للكمبيوتر إذ أن مسرح الجريمة في هذه الحالة يحتوي علي الأدلة المادية التي تدل دلالة واضحة علي وقوع الجريمة ونسبتها لشخص معين، فيقومون بعد ذلك بوضع الأختام وضبط الأدلة وإخطار النيابة العامة.

---

(1) الموقع والمرجع السابق.

أما الصعوبات الحقيقية التي تواجه رجال الضابطة العدلية علي هذا الصعيد، فتظهر عندما تكون الجريمة واقعة علي برامج الكمبيوتر وبياناته أو بواسطتها وذلك بالنظر إلي قلة الآثار المادية التي قد تنتج عن هذا من الجرائم وكثرة عدد الأشخاص الذين قد يترددون علي مسرح الجريمة خلال المدة الفاصلة بين وقوع الجريمة والكشف عنها<sup>(١)</sup>.

• ويوصي<sup>(٢)</sup>، في هذا الإطار، حفاظا علي مسرح الجريمة، بما يأتي:

- تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة وأخذ صورة لأجزائه الخلفية وسائر ملحقاته.
- ملاحظة طريقة إعداد نظام الكمبيوتر بعناية بالغة.
- إثبات الحالة التي تكون عليها توصيلات وكابلات الكمبيوتر والمتصلة بمكونات النظام.
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة خشية إتلاف البيانات المخزنة.

• التفتيش عن أدلة الجريمة المعلوماتية<sup>(٣)</sup>:

إذا كانت الجريمة واقعة علي المكونات المادية للكمبيوتر، فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش، أما إذا كانت الجريمة واقعة علي برامج الحاسب وبياناته، فإن الصعوبات تبرز علي اعتبار أنه بإمكان الجاني التخلّص من البيانات التي يستهدفها التفتيش عبر إرسالها من خلال نظام معلوماتي من مكان إلي آخر، وعلي اعتبار أن التفتيش عن هذه البيانات

(١) الموقع والمرجع السابق.

(٢) حول قرار قاضي التحقيق في بيروت، جريدة السفير العدد الصادر بتاريخ ١٨/١١/١٩٩٩، وحول قرار قاضي التحقيق في جبل لبنان، نشرة قضائية للبنانية ١٩٧١ ص ٤٨٨.

(٣) القاضي وليد عاكوم التحقيق في جرائم الحاسوب. الموقع والمرجع السابق.



يستوجب الكشف عن الرقم السري Code للمرور الي منغات البيانات، وهذا الرقم السري يعرفه المتهم، ولا يمكن إجباره علي البوح به.

ومن أجل تخطي هذه الصعوبات، يجب برأينا أن لا يكون الإنز بالتفتيش محددا بمكان معين، بل يجب أن يستند إلي تفتيش أي نظام ألي موجود في مكان آخر بغية التوصل إلي بيانات يمكن أن تفيد بشكل معقول في الكشف الحقيقة، شرط عدم انتهاك سيادة دولة أخرى وأن يحل قاضي التحقيق محل الشخص، صاحب المكان، المراد تفتيشه بصورة مؤقتة.

كما يجب أن يتضمن إذن التفتيش الأجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات<sup>(1)</sup>.

#### \* ضبط الأدلة:

الضبط، بحسب الأصل، لا يرد إلا علي أشياء مادية، فلا صعوبة بالتالي بضبط أدلة الجريمة الواقعة علي المكونات المادية للكمبيوتر، كرفع البصمات مثلا عنها.

وذلك، فلا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخه غير المشروع أو إتلافه بوسائل تقليدية كالكرس أو الحرق.

ولكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس، وفي ضبط بيانات الكمبيوتر Data لعدم وجود أي دليل مرئي في هذه الحالات ولسهولة تدمير الدليل في ثوان معدومة ولعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات.

---

(1) قرار محكمة الجنايات منشور في مجلة العدل اللبنانية ٢٠٠٠ ص ٣٧٥.

وباستنظار استحداث قوانين تتضمن مفاهيم قانونية عامة وجديدة نقترح  
علي هذا الصعيد ما يأتي:

- تشجيع المجني عليها بالإبلاغ عن هذه الجرائم فور ملاحظتها.
- حث العاملين علي النظام المعلوماتي علي معاونة السلطة لضبط البيانات.
- ضرورة اتباع القواعد الفنية اللازمة لحماية البيانات وتجنبيها خطر الإتلاف.
- منح أوسع الصلاحيات لسلطة التحقيق لاختراق نظام الكمبيوتر وضبط ما يحويه من بيانات مخزنة دون إخطار مسبق بعملية التفتيش والضبط.

#### ب- دور السلطة القضائية:

علي اعتبار أن القاضي هو حامي الحقوق والحريات، فإنه يجب أن يلعب دورا هاما في قمع الجرائم المعلوماتية.

وتفعيلا لهذا الدور، يجب علي القاضي أن يكون متفهما لفحوى التقدم التقني وما ينتج عنها من وسائل إجرامية يغلب عليها الطابع التقني.

وعلي هذا الأساس، ينبغي أن يقبل بالأدلة المستمدة من الكمبيوتر لإثبات وقائع الدعوى التي تتناول جرائم المعلوماتية، ويساعده في هذا الأمر مبدأ الإثبات الحر والقناعة الشخصية للقاضي في مجال الجنائي.

ومن ناحية أخرى، فإنه يجب أن يتحلي بالمقدرة علي التكيف القانوني للأفعال الجرمية المستحدثة مع التشريعات التجريبية القائمة.

#### ٢- بعض التطبيقات القانونية والقضائية:

نعرض الآن الواقع القانوني والقضائي الذي يعالج الجرائم المعلوماتية كالآتي:

#### أ- القوانين المطبقة:

تتطلب الجرائم الواقعة علي الأنظمة المعلوماتية أحكاما ونصوصا تجريبية خاصة بها.

وعليه، فقد بادرت العديد من الدول الغربية إلي وضع نصوص ومواد جزائية تعاقب صراحة الجرائم المعلوماتية، في حين أن القوانين في الدول العربية وفي لبنان خصوصا لم تتطرق بعد إلي هذه الفئة من الجرائم.

#### • في القانون اللبناني:

أن القانون اللبناني الوضعي الحالي لا يتطرق أبدا إلي الجرائم المعلوماتية بشكل مباشر، ولا تزال الدعاوى المتعلقة بهذه الجرائم تستند إلي المواد الجزائية المنصوص عنها في قانون العقوبات.

فالتجسس معاقب عليه في قانون العقوبات اللبناني من المادة ٢٨١ لغاية المادة ٢٨٤ عندما يطال المعلومات المتعلقة بسلامة الدولة فقط، ولا يتحدث عن حالات التجسس الصناعي أو علي الأفراد، ولا يتمكن بالتالي التوسع في تفسير النص وجعله شاملا لهذه الحالات لأن القانون الجزائي يفسر بصورة ضيقة انطلاقا من مبدأ لا عقوبة دون نص.

أما التشويش والتخريب في أنظمة المعلومات، فيمكن الاستعانة بنص المادة ٧٣٣ عقوبات التي تعاقب كل من خرب قصدا شيئا يخص غيره بالغرامة وبالحبس لغاية ستة أشهر، ولكن هذا النص يتعلق فقط بالأشياء الملموسة كأجهزة الكمبيوتر وتوابعها، ولا يتطرق إلي قضية التشويش والتجريب علي المعلومات التي تحتويها.

أما المادة ٦٣٥ عقوبات، فتعرف السرقة بأنها أخذ مال الغير المنقول خفية أو عنوه يقصد التملك، وتنزل الطاقات المحرزة منزلة الأشياء المنقولة في تطبيق هذا النص، ويستنتج من ذلك بأنه يمكن، بالاستناد إلي المادة

المذكورة، معاقبة سارق جهاز الكمبيوتر كآلة، ولكن لا يمكن معاقبة سرقة المعلومات التي هي أشياء غير ملموسة.

أما الابتزاز باستعمال معلومات أمكن الحصول عليها عبر الأنظمة المعلوماتية، فتقع ضمن نطاق تطبيق نص المادة ٦٥٠ عقوبات لأن النص المذكور لا يشير إلى مصدر المعلومات التي تستعمل في التهويل والابتزاز.

وأن العقوبات الواردة في المادتين ٤٧١ و ٤٥٤ عقوبات تظال تزوير بطاقات الاعتمادات المصرفية واستعمالها كمستند - أما تزوير المعلومات أي تبديل الحقيقة على الشرائط المغنطة وفي مجموعة البيانات أي على المضمون الذهني للبرامج، فلا يقع تحت أحكام هاتين المادتين لانتهاء وجود المستند بالمعنى القانوني الوارد فيهما.

وبتاريخ ١٣/٤/١٩٩٩، صدر قانون متعلق بحماية الملكية الأدبية والفنية يحمل الرقم ٧٥ ويعد هذا القانون إنجازا كبيرا في هذا المجال إذ إنها المرة الأولى التي تعاقب بها الجرائم المعلوماتية بنص صريح.

فالمادة الأولى من القانون المذكور عرفت برنامج الحاسب الآلي بما حرفيته، أنه مجموعة من الأوامر معبر عنها بكلمات أو برموز أو بأي شكل آخر بإمكانها عندما تدخل في مادة يمكن للحاسب أن يقرأها أن تجعل الحاسب الآلي يؤدي أو ينفذ مهمة ما أو يعطي نتيجة ما.

كذلك، ورد في المادة الأولى تعريف لمسألة نقل المعلومات إلى الجمهور التي يمكن أن تكون موضوع مسألة إذا تناولت أعمالا مشمولة بالحماية وإذا جرت بواسطة وسائل سلكية أو لا سلكية عن طريق الإنترنت.

واعتبر هذا القانون في المادة الثانية منه برامج الحاسب الآلي، مهما كانت لغات هذه البرامج، وكذلك الأعمال التحضيرية لهذه البرامج من ضمن الأعمال المشمولة بالحماية.

وقد أقرت المادتان ٨٥ و ٨٦ منه العقوبات اللازمة علي كل من يتعدى علي هذه البرامج.

**\* في قوانين الدول الغربية:**

تعتبر فرنسا من بين أولى الدول التي أصدرت تشريعا خاصا في مجال الجرائم المعلوماتية بموجب قانونين: الأول، بتاريخ ١٩٦٨/١/٥ حول المعلوماتية والحريات، والثاني، فهو قانون God rain حول الغش المعلوماتية الصادر بتاريخ ١٩٨٨/١/٥.

ومن بين الاعتداءات التي أعطيت وصفا جرميا يعاقب عليه بالسجن وبغرامات مرتفعة، الدخول أو البقاء غير المشروع داخل النظام المعلوماتية، والاعتداءات علي المعلومات داخل الأنظمة، وجرائم التزوير في المعلوماتية، وتآليف جمعيات الأشرار المعلوماتين، وإدخال جرائم أو ديدان أو إلقاء قنابل منطقة أو أحصنة طروادة وغيرها.



**الفصل الخامس**  
**الاتفاقيات الدولية علي**  
**المستوى الدولي**  
**وعلي المستوى الإقليمي**  
**للدول العربية**





**أولا**  
**اتفاقية برن لحماية**  
**المصنفات الأدبية والفنية**



اتفاقية برن لحماية المصنفات الأدبية والفنية

المؤرخة ٢٤ يولية / تموز ١٩٧١

والمعدلة في ٢٨ سبتمبر / أيلول ١٩٧٩

المنظمة العالمية للملكية الفكرية جنيف ١٩٩٨

اتفاقية برن لحماية المصنفات الأدبية والفنية

المؤرخة ٩ سبتمبر / أيلول ١٨٨٦، والمكملة بباريس في ٤ مايو / أيار ١٨٩٦، والمعدلة ببرلين في ١٣ نوفمبر / تشرين الثاني ١٩٠٨، والمكملة ببرن في ٢٠ مارس / آذار ١٩١٤، والمعدلة بروما في ٢ يولية / حزيران ١٩٢٨ وبروكسل في ٢٦ يولية / حزيران ١٩٤٨ واستكهولم في ١٤ يولية / تموز ١٩٦٧ وباريس في ٢٤ يولية / تموز ١٩٧١ والمعدلة في ٢٨ سبتمبر / أيلول ١٩٧٩

إن دول الاتحاد، إذ تحدها الغربية علي حد سواء في حماية حقوق المؤلفين علي مصنفاتهم الأدبية والفنية بأكثر الطرق الممكنة فعالية واتساقا. واعترافا منها بأهمية أعمال مؤتمر إعادة النظر الذي انعقد في استكهولم عام ١٩٦٧،

قررت تعديل الوثيقة التي أقرها مؤتمر استكهولم، مع الإبقاء علي المواد من ١ إلي ٢٠ والمواد من ٢٢ إلي ٢٦ من تلك الوثيقة دون تغيير. تبعا لذلك فإن المندوبين المفوضين الموقعين أدناه، بعد تقديمهم وثائق تفويضهم الكامل والتي وجدت صحيحة ومستوفاة للشكل القانوني، قد اتفقوا علي ما يلي:

## مادة ١

### إنشاء اتحاد

تشكل الدول التي تسري عليها هذه الاتفاقية اتحادا لحماية حقوق المؤلفين علي مصنفاتهم الأدبية والفنية.

## مادة ٢

(المصنفات المتمتعة بالحماية: (١) "المصنفات الأدبية والفنية" (٢) إمكانية المطالبة بالتحديد (٣) المصنفات المشتقة (٤) النصوص الرسمية (٥) المجموعات (٦) التزام الحماية، المستفيدون من الحماية (٧) مصنفات الفنون التطبيقية والرسوم والنماذج الصناعية (٨) الأخبار اليومية)

(١) "تشمل عبارة المصنفات الأدبية والفنية" كل إنتاج في المجال الأدبي والعلمي والفني أيا كانت طريقة أو شكل التعبير عنه مثل الكتب والكتيبات وغيرها من المحررات، والمحاضرات والخطب والمواعظ والأعمال الأخرى التي تنتم بنفس الطبيعة، والمصنفات المسرحية أو المسرحيات الموسيقية، والمصنفات التي تؤدي بحركات أو خطوات فنية والتمثيلات الإيمائية، والمؤلفات الموسيقية سواء اقترنت بالألفاظ أو لم تقترن بها، والمصنفات السينمائية ويقاس عليها المصنفات التي يعبر عنها بأسلوب مماثل للأسلوب السينمائي، والمصنفات الخاصة بالريم والتصوير بالخطوط أو بالألوان وبالعمارة وبالنحت وبالحفر وبالطباعة علي الحجر، والمصنفات الفوتوغرافية ويقاس علي المصنفات التي يعبر عنها بأسلوب مماثل للأسلوب الفوتوغرافي، والمصنفات الخاصة بالفنون التطبيقية، والصور التوضيحية والخرائط الجغرافية والتصميمات والرسومات التخطيطية والمصنفات المجسمة المتعلقة بالجغرافيا أو الطبوغرافيا أو العمارة أو العلوم.

- (٢) تختص، مع ذلك تشريعات دول الاتحاد بحق القضاء بأن المصنفات الأدبية والفنية أو مجموعة أو أكثر منها لا تتمتع بالحماية طالما أنها لم تتخذ شكلا ماديا معيناً.
- (٣) تتمتع الترجمات والتحويلات والتعديلات الموسيقية وما يجري على المصنف الأدبي أو الفني من تحويلات أخرى بنفس الحماية التي تتمتع بها المصنفات الأصلية وذلك دون المساس بحقوق مؤلف المصنف الأصلي.
- (٤) تختص تشريعات دول الاتحاد بتحديد الحماية التي تمنحها للنصوص الرسمية ذات الطبيعة التشريعية أو الإدارية أو القضائية وكذلك للترجمة الرسمية لهذه النصوص.
- (٥) تتمتع مجموعات المصنفات الأدبية أو الفنية لدوائر المعارف والمختارات الأدبية التي تعتبر ابتكاراً فكرياً، بسبب اختيار وترتيب محتوياتها، بالحماية بهذه الصفة وذلك دون المساس بحقوق المؤلفين فيما يختص بكل مصنف بشكل جزءاً من هذه المجموعات.
- (٦) تتمتع المصنفات المذكورة آنفاً بالحماية في جميع دول الاتحاد. وتباشر هذه الحماية لمصلحة المؤلف ولمصلحة من آل إليه الحق من بعده.
- (٧) تختص تشريعات دول الاتحاد بتحديد مجال تطبيق القوانين الخاصة بمصنفات الفنون التطبيقية والرسوم والنماذج الصناعية، وكذلك شروط حماية هذه المصنفات والرسوم والنماذج، وذلك مع مراعاة أحكام المادة ٧ (٤) من هذه الاتفاقية، وبالنسبة للمصنفات التي تتمتع بالحماية في دولة المنشأة بصفتها فقط رسوم ونماذج، فإنه لا يكون من حقها التمتع في دولة أخرى من دول الاتحاد إلا بالحماية الخاصة المقررة في تلك الدولة للرسوم والنماذج. ومع ذلك، فإذا لم تكن مثل هذه الحماية الخاصة مقررة في تلك الدولة الأخيرة، فإن هذه المصنفات تتمتع بالحماية باعتبارها مصنفات فنية.

(٨) لا تنطبق الحماية المقررة في هذه الاتفاقية علي الأخبار اليومية أو علي الأحداث المختلفة التي تتصف بكونها مجرد معلومات صحفية.

#### مادة ٢ (ثانيا)

(إمكانية تحديد حماية بعض المصنفات: (١) بعض الخطب (٢) بعض استعالات المحاضرات والخطب (٣) الحق في عمل مجموعة من هذه المصنفات (١) تختص تشريعات دول الاتحاد بالحق في أن تستبعد جزئيا أو كليا الخطب السياسية والمرافعات التي تتم أثناء الإجراءات القضائية من الحماية المقررة في المادة السابقة.

(٢) تختص أيضا تشريعات دول الاتحاد بحق تحديد الشروط التي يمكن بمقتضاها نقل المحاضرات والخطب والأعمال الأخرى التي تتسم بنفس الطبيعة والتي تلقى علنيا وذلك عن طريق الصحافة وإذاعتها وإحاطة الجمهور علما بها بالوسائل السليكية أو عن طريق تضمينها وسائل النقل للجمهور المنصوص عليها في المادة ١١ (ثانيا) (١) من هذه الاتفاقية وذلك عندما يبرر الهدف الإعلامي المنشود مثل هذا الاستعمال.

(٣) ومع ذلك، يتمتع المؤلف بحق استثنائي في عمل مجموعة من مصنفاته المنصوص عليها في الفقرات السابقة.

#### مادة ٣

(معايير الحماية: (١) جنسية المؤلف، مكان نشر المصنف (٢) محل إقامة المؤلف (٣) المصنفات "المنشورة" (٤) المصنفات "المنشورة في آن واحد" (١) تشمل الحماية المنصوص عليها في هذه الاتفاقية: (أ) المؤلفين من رعايا إحدى دول الاتحاد عن مصنفاتهم سواء كانت منشورة أم لم تكن.

(ب) المؤلفين من غير رعايا إحدى دول الاتحاد، عن مصنفاتهم التي تنشر لأول مرة في إحدى دول الاتحاد أو في آن واحد في دول خارج الاتحاد وفي إحدى دول الاتحاد.

(٢) في تطبيق أحكام هذه الاتفاقية يعامل المؤلفين من غير رعايا إحدى دول الاتحاد الذين تكون إقامتهم العادية في إحدى هذه الدول معاملة المؤلفين من رعايا تلك الدولة.

(٣) "يقصد بتعبير المصنفات المنشورة" المصنفات التي تنشر بموافقة مؤلفيها أيا كانت وسيلة عمل النسخ، بشرط أن يكون توافر هذه النسخ قد جاء علي نحو يفي بالاحتياجات المعقولة للجمهور مع مراعاة طبيعة المصنف، ولا بعد نشرها تمثيل مصنف مسرحي أو مصنف مسرحي موسيقي أو سينمائي وأداء مصنف موسيقي والقراءة العلنية لمصنف أدبي والنقل السلبي أو إذاعة المصنفات الأدبية أو الفنية وعرض مصنف فني وتنفيذ مصنف معماري.

(٤) يعتبر كأنه منشور في آن واحد في عدة دول كل مصنف ظهر في دولتين أو أكثر خلال ثلاثين يوما من تاريخ نشره لأول مرة.

#### مادة ٤

(معايير حماية المصنفات السينمائية والمصنفات المعمارية وبعض مصنفات الفنون التخطيطية والتشكيلية

تسري الحماية المقررة في هذه الاتفاقية حتى إذا لم تتوفر الشروط الواردة في المادة ٣ وذلك علي:

(أ) مؤلفي المصنفات السينمائية التي يكون مقر منتجها أو محل إقامته المعتادة في إحدى دول الاتحاد.

(ب) مؤلفي المصنفات المعمارية المقامة في إحدى دول الاتحاد أو المصنفات الفنية الأخرى الداخلة في مبني أو إنشاء آخر كائن في إحدى دول الاتحاد.

## مادة ٥

(الحقوق المضمونة: (١) و (٢) خارج دولة المنشأ (٣) في دولة المنشأ (٤) دولة المنشأ")

(١) يتمتع المؤلفون، في دول الاتحاد غير دولة منشأ المصنف، بالحقوق التي تخولها قوانين تلك الدول حالياً أو قد تخولها مستقبلاً لرعاياها بالإضافة إلى الحقوق المقررة بصفة خاصة في هذه الاتفاقية، وذلك بالنسبة للمصنفات التي يتمتعون علي أساسها بالحماية بمقتضى هذه الاتفاقية.

(٢) لا يخضع التمتع أو ممارسة هذه الحقوق لأي إجراء شكلي، فهذا التمتع وهذه الممارسة مستقلان عن وجود الحماية في دولة منشأ المصنف، تبعاً لذلك، فإن نطاق الحماية وكذلك وسائل الطعن المقررة للمؤلف لحماية حقوقه بحكمها تشريع الدولة المطلوب توفير الحماية فيها دون سواه، وذلك بصرف النظر عن أحكام هذه الاتفاقية.

(٣) الحماية في دولة المنشأ يحكمها التشريع الوطني. ومع ذلك إذا كان المؤلف من غير رعايا دولة منشأ المصنف الذي يتمتع علي أساسه بالحماية بمقتضى هذه الاتفاقية، فإنه يتمتع في تلك الدولة بذات الحقوق المقررة لرعاياها.

(٤) تعتبر دولة المنشأ:

(أ) بالنسبة للمصنفات التي تنشر لأول مرة في إحدى دول الاتحاد، الدولة المذكورة، وفي حالة المصنفات التي تنشر في آن واحد في عدد من دول الاتحاد التي تمنح مدداً مختلفة للحماية، الدولة التي يمنح تشريعها مدة الحماية الأقصر.



(ب) بالنسبة للمصنفات التي تنشر في أن واحد في دولة خارج الاتحاد ودولة من دول الاتحاد، الدولة الأخيرة.

(ج) بالنسبة للمصنفات غير المنشورة أو بالنسبة للمصنفات التي تنشر لأول مرة في دولة خارج الاتحاد دون أن تنشر في أن واحد في دولة من دول الاتحاد، دولة الاتحاد التي يعتبر المؤلف من رعاياها ومع ذلك:

(١) إذا ما تعلق الأمر بمصنفات سينمائية يقع بمقر منتجها أو محل إقامته المعتادة في دولة من دول الاتحاد، فإن هذه الدولة تكون دولة المنشأ.

(٢) إذا ما تعلق الأمر بمصنفات معمارية مقامة في إحدى بلدان الاتحاد أو مصنفات فنية أخرى داخلية في مبني أو إنشاء آخر يقع في إحدى بلدان الاتحاد، فإن هذه الدولة تكون دولة المنشأ.

## مادة ٦

(إمكانية تقييد الحماية بالنسبة لبعض مصنفات رعايا بعض الدول خارج الاتحاد: (١) في الدولة التي تم النشر فيها لأول مرة وفي الدول الأخرى (٢) عدم رجعية القيود (٣) الإخطار)

(١) عندما لا تقرر دولة خارج الاتحاد الحماية الكافية لمصنفات مؤلفين من رعايا دولة من دول الاتحاد فلهذه الأخيرة أن تقيّد من حماية مصنفات المؤلفين الذين كانوا في تاريخ أول نشر من رعايا تلك الدولة دون أن يقيموا عادة في إحدى دول الاتحاد. فإذا ما استعملت دولة أول نشر هذا الحق فلا يتطلب من دول الاتحاد الأخرى منح مثل هذه المصنفات التي تخضع لمعاملة خاصة، حماية أوسع من تلك التي تمنح لها في دولة أول نشر.

(٢) لا تؤثر القيود المقررة بموجب الفقرة السابقة على الحقوق التي يكون المؤلف قد اكتسبها بالنسبة لمصنف نشر في إحدى دول الاتحاد من وضع هذه القيود موضع التنفيذ.

(٣) علي دول الاتحاد التي تضع قيودا علي حماية حقوق المؤلفين طبقا لأحكام هذه المادة، أن تخطر ذلك إلي المدير العام للمنظمة العالمية للملكية الفكرية (ويشار إليه فيما بعد باسم "المدير العام") بموجب إعلان كتابي تحدد فيه الدول التي تقيد الحماية في مواجهتها وكذا القيود التي تخضع لها حقوق المؤلفين من رعاياها هذه الدول. ويقوم المدير العام بإبلاغ هذا الإعلان في الحال إلي جميع دول الاتحاد.

#### مادة ٦ (ثانيا)

(الحقوق المعنوية: (١) الحق في المطالبة بنسبة المصنف لمؤلفه،  
الحق في الاعتراض علي إدخال بعض التعديلات علي المصنف والمساس  
به (٢) بعد وفاة المؤلف (٣) وسائل الطعن)

(١) بغض النظر عن الحقوق المالية للمؤلف، بل وحتى بعد انتقال هذه الحقوق، فإن المؤلف يحتفظ بالحق في المطالبة بنسبة المصنف إليه، وبالاعتراض علي كل تخريب أو تشويه أو أي تعديل آخر لهذا المصنف أو كل مساس آخر بذات المصنف يكون ضارا بشرفه أو بسمعته.

(٢) الحقوق الممنوحة للمؤلف بمقتضى الفقرة (١) السابقة تظل محفوظة بعد وفاته، وذلك علي الأقل حين انقضاء الحقوق المالية، ويمارس هذه الحقوق الأشخاص أو الهيئات المصرح بها من قبل تشريع الدولة المطلوب توفير الحماية فيها. ومع ذلك، فإن الدول التي لا يتضمن تشريعها المعمول به، عند التصديق علي هذه الاتفاقية أو الانضمام إليها، نصوصا تكفل الحماية بعد وفاة المؤلف لكل الحقوق المنصوص عليها في الفقرة السابقة، يكون لها الحق في النص علي أن بعض هذه الحقوق لا يحتفظ بها بعد وفاة المؤلف.

(٣) وسائل الطعن للمحافظة علي الحقوق المقررة في هذه المادة يحددها تشريع الدولة المطلوب توفير الحماية فيها.

## مادة ٧

(مدة الحماية: (١) بوجه عام (٢) بالنسبة للمصنفات السينمائية (٣) بالنسبة للمصنفات التي تحمل اسم المؤلف أو تحمل اسما مستعاراً (٤) بالنسبة لمصنفات التصوير الفوتوغرافي ومصنفات الفنون التطبيقية (٥) تاريخ بدء احتساب مدة الحماية (٦) منح مدد أطول (٧) منح مدد أقصر (٨) التشريعات المطبقة، "مقارنة" المدد)

(١) مدة الحماية التي تمنحها هذه الاتفاقية تشمل مدة حياة المؤلف وخمسين سنة بعد وفاته.

(٢) ومع ذلك، فإنه بالنسبة للمصنفات السينمائية، يكون لدول الاتحاد الحق في أن تنص على أن مدة الحماية تنتهي بمضي خمسين عاماً على وضع المصنف في متناول الجمهور بموافقة المؤلف، وفي حالة عدم تحقق مثل هذا الحدث خلال خمسين عاماً من تاريخ إنجاز مثل هذا المصنف، فإن مدة الحماية تنقضي بمضي خمسين عاماً على هذا الإنجاز.

(٣) بالنسبة للمصنفات التي لا تحمل اسم المؤلف أو تحمل اسماً مستعاراً، فإن مدة الحماية التي تمنحها هذه الاتفاقية تنتهي بمضي خمسين سنة على وضع المصنف في متناول الجمهور بطريقة مشروعة، ومع ذلك، إذا كان الاسم المستعار الذي يتخذه المؤلف لا يدع أي مجال للشك في تحديد شخصيته فإن مدة الحماية تكون هي المنصوص عليها في الفقرة (١). وإذا كشف مؤلف مصنف يعوزه اسم المؤلف أو يحمل اسماً مستعاراً عن شخصيته خلال المدة المذكورة أعلاه، تكون مدة سريان الحماية هي المدة المنصوص عليها في الفقرة (١). ولا تلتزم دول الاتحاد بحماية المصنفات التي لا تحمل اسم مؤلفها أو تحمل اسماً مستعاراً إذا كان هناك سبباً معقولاً لافتراض أن مؤلفها قد توفي منذ خمسين سنة.

(٤) تختص شريعات دول الاتحاد بحق تحديد مدة حماية مصنفات التصوير الفوتوغرافي ومصنفات الفن التطبيقي بالقدر الذي تتمتع فيه بالحماية كمصنفات فنية، ومع ذلك فإن هذه المدة لا يمكن أن تقل عن خمس وعشرين سنة تبدأ من تاريخ إنجاز مثل هذا المصنف.

(٥) يبدأ سريان مدة الحماية المقررة علي أثر وفاة المؤلف، وكذلك المدد المقررة في الفقرات (٢) و (٣) و (٤) أعلاه، من تاريخ الوفاة أو حصول الواقعة المشار إليها في تلك الفقرات، علي أن سريان هذه المدد يبدأ دائما احتسابه اعتبارا من أول يناير من السنة التالية للوفاة أو حصول الواقعة.

(٦) يمكن لدول الاتحاد أن تقرر مدة للحماية أطول من تلك المنصوص عليها في الفقرات السابقة.

(٧) يكون لدول الاتحاد الملزمة بأحكام وثيقة روما من هذه الاتفاقية والتي تمنح تشريعاتها الوطنية السارية المفعول وقت توقيع هذه الوثيقة مدد أقل من المنصوص عليها في الفقرات السابقة، حق الإبقاء علي تلك المدد عند التصديق علي هذه الوثيقة أو الانضمام إليها.

(٨) وعلي كل الأحوال فإن المدة يحكمها تشريع الدولة المطلوب توفير الحماية فيها، ومع ذلك، وما لم يقرر تشريع هذه الدولة غير ذلك، فإن المدة لن تتجاوز المدة المحددة في دولة منشأ المصنف.

#### مادة ٧ (ثانيا)

(مدة حماية المصنفات التي اشترك في وضعها أكثر من مؤلف واحد)

تطبق أحكام المادة السابقة أيضا في الحالة التي يكون فيها حق المؤلف مملوكا علي الشيوع للشركاء في عمل مصنف، علي أن تحسب للمدد المقررة علي أثر وفاة المؤلف اعتبارا من تاريخ آخر من بقي من الشركاء علي قيد الحياة.

## مادة ٨

### (حق الترجمة)

يتمتع مؤلفو المصنفات الأدبية والفنية الذين تحميهم هذه الاتفاقية بحق استثنائي في ترجمة أو التصريح بترجمة مصنفاتهم طوال مدة حماية ما لهم من حقوق في المصنفات الأصلية.

## مادة ٩

(حق النسخ: (١) بوجه عام (٢) إمكانية وضع استثناءات (٣) التسجيلات الصوتية والبصرية)

(١) يتمتع مؤلفو المصنفات الأدبية والفنية الذين تحميهم هذه الاتفاقية بحق استثنائي في التصريح بعمل نسخ من هذه المصنفات بأية طريقة وبأي شكل كان.

(٢) تختص تشريعات دول الاتحاد بحق السماح بعمل نسخ من هذه المصنفات في بعض الحالات الخاصة بشرط ألا يتعارض عمل مثل هذه النسخ مع الاستغلال العادي للمصنف normal exploitation وألا يسبب ضرراً بغير مبرر للمصالح المشروعة للمؤلف. " legitimate interest of the author

(٣) كل تسجيل صوتي أو بصري يعتبر نقلاً في مفهوم هذه الاتفاقية.

## Article 9

( Right of Reproduction: 1. Generally; 2 Possible exceptions; 3. sound and visual recordings)

(1) Authors of literary and artistic works protected by this convention shall have the exclusive right of authorizing the reproduction of these works, in any manner of from.

(2) It shall be a matter for legislation in the countries of the union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author.

(3) Any sound or visual recording shall be considered as a reproduction for the purposes of this Convention.

## مادة ١٠

(حرية استعمال المصنفات Free uses of Works في بعض الحالات:

(١) المقتطفات (٢) التوضيح في الأغراض التعليمية (٣) ذكر المصدر واسم المؤلف)

(١) يسمح بنقل مقتطفات quotations من المصنف الذي وضع في متناول الجمهور علي نحو مشروع، بشرط أن يتفق ذلك وحسن الاستعمال وأن يكون في الحدود التي يبررها الغرض المنشود، ويشمل ذلك نقل مقتطفات من مقالات الصحف والدوريات في شكل مختصرات صحفية.

(٢) تختص تشريعات دول الاتحاد، والاتفاقات الخاصة المعقودة أو التي قد تعقد فيما بينها، وفي حدود ما يبرره الغرض المنشود، بإباحة استعمال المصنفات الأدبية أو الفنية علي سبيل التوضيح للأغراض التعليمية وذلك عن طريق النشرات والإذاعات اللاسلكية والتسجيلات الصوتية أو البصرية بشرط أن يتفق مثل هذا الاستخدام وحسن الاستعمال.

(٤) يجب عند استعمال المصنفات طبقاً للفقرتين السابقتين من هذه المادة ذكر المصدر واسم المؤلف إذا كان وأراد به.

## Article 10

(Certain Free uses of Works: 1. Quotations; 2. Illustrations for teaching; 3. Indication of source and author).

(1) It shall be permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries.

(2) It shall be a matter for legislation in the countries of the Union, and for special agreements existing or to be concluded between them, to them, to permit the utilization, to the extent justified by the purpose, of literary or artistic works by way of illustration in publications, broadcasts or sound or visual recordings for teaching, provided such utilization is compatible with fair practice.

(3) Where use is made of works in accordance with the preceding paragraphs of this Article, mention shall be made of the source, and of the source, and of the name of the author if it appears thereon.

#### **مادة ١٠ (ثانياً)**

(إمكانيات أخرى بشأن حرية استعمال المصنفات: (١) بعض المقالات وكذلك بعض المصنفات المذاعة (٢) المصنفات التي تشاهد أو تسمع أثناء عرض أحداث جارية)

(١) تختص تشريعات دول الاتحاد بحق السماح بنقل المقالات المنشورة في الصحف والدوريات عن موضوعات جارية اقتصادية أو سياسية أو دينية أو المصنفات المذاعة التي لها ذات الطابع، وذلك بواسطة الصحافة أو الإذاعة أو النقل السلبي للجمهور، في الحالات التي لا تكون فيها حقوق النقل أو الإذاعة أو النقل السلبي المذكور محفوظة صراحة، ومع ذلك فإنه يجب دائماً الإشارة بكل وضوح إلى المصدر، ويحدد تشريع الدولة المطلوب توفير الحماية فيها الجزاء المترتب على الإخلال بهذا الالتزام.

(٢) تختص أيضا تشريعات دول الاتحاد بتحديد الشروط التي يمكن بمقتضاها، وذلك بمناسبة عرض أحداث جارية عن طريق التصوير الفوتوغرافي أو السينمائي أو الإذاعة أو النقل السلبي للجمهور، نقل المصنفات الأدبية أو الفنية التي شوهدت أو سمعت أثناء الحدث وجعلها في متناول الجمهور وذلك في حدود ما يبرره الغرض الإعلامي المنشود.

#### Article 10 bis

**(Further possible free Uses of Works: 1. Of certain articles and broadcast works; 2. of works seen or heard in connection with current events).**

(1) It shall be a matter for legislation in the countries of the Union to permit the reproduction by the press, the broadcasting or the communication to the public by wire of articles published in newspapers or periodicals on current economic, political or religious topics, and of broadcast works of the same character, in cases in which the reproduction, broadcasting or such communication thereof is not expressly reserved. Nevertheless, the source must always be clearly indicated; the legal consequences of a breach of this obligation shall be determined by the legislation of the country where protection is claimed.

(2) It shall also be a matter for legislation in the countries of the Union to determine the conditions under which, for the purpose of reporting current events by means of photography, cinematography, broadcasting or communication to the public by wire, literary or artistic works seen or heard in the course of the event may, to the extent justified by the informative purpose, be reproduced and made available to the public.

#### مادة ١١

(بعض الحقوق المتعلقة بالمصنفات المسرحية والموسيقية، حق التمثيل أو الأداء العلني ونقل تمثيل أو أداء إلى الجمهور (٢) بالنسبة للترجمات)



- (١) يتمتع مؤلفو المصنفات المسرحية والمسرحيات الموسيقية والمصنفات الموسيقية بحق استثنائي في التصريح:
- (١) بتمثيل مصنفاتهم وأدائها علنا بما في ذلك التمثيل والأداء العلني بكل الوسائل أو الطرق.
- (٢) بنقل تمثيل وأداء مصنفاتهم إلى الجمهور بكل الوسائل.
- (٢) يتمتع مؤلفو المصنفات المسرحية أو المسرحيات الموسيقية طوال مدة سريان حقوقهم على المصنف الأصلي بنفس الحقوق فيما يختص بترجمة مصنفاتهم.

#### مادة ١١ (ثانيا)

- (حقوق الإذاعة والحقوق المرتبطة بها: (١) الإذاعة وغيرها من وسائل النقل اللاسلكي، نقل المصنف المذاع إلى الجمهور سلكيا أو لا سلكيا، نقل المصنف المذاع إلى الجمهور سواء بمكبر للصوت أو بأي جهاز مشابه آخر (٣) التراخيص الإجبارية (٣) التسجيل، التسجيلات المؤقتة)
- (١) يتمتع مؤلفو المصنفات الأدبية والفنية بحق استثنائي في التصريح:
- (١) بإذاعة مصنفاتهم أو بنقلها إلى الجمهور بأية وسيلة أخرى تستخدم لإذاعة الإشارات أو الأصوات أو الصور باللاسلكي.
- (٢) بأي نقل للجمهور، سلكيا كان أم لا سلكيا، للمصنف المذاع عندما تقوم بهذا النقل هيئة أخرى غير الهيئة الأصلية.
- (٣) بنقل المصنف المذاع للجمهور بمكبر للصوت أو بأي جهاز آخر مشابه ناقل للإشارات أو الأصوات أو الصور.
- (٢) تختص تشريعات دول الاتحاد بتحديد شروط استعمال الحقوق المذكورة في الفقرة (١) السابقة، علي أن يقتصر أثر هذه الشروط على الدول

التي فرضتها لا غير، ولا يمكن أن تمس هذه الشروط بأي حال بالحقوق المعنوية للمؤلف، ولا بحقه في الحصول على مقابل عادل تحدده السلطة المختصة في حالة عدم الاتفاق عليه وديا.

(٣) ما لم ينص علي خلاف ذلك، فإن التصريح الممنوح طبقا للفقرة (١) من هذه المادة، لا يتضمن التصريح بتسجيل المصنف المذاع بالآلات تسجيل الأصوات أو الصور. ومع ذلك فإن تشريعات دول الاتحاد تختص بتحديد نظام التسجيلات المؤقتة التي تجريها هيئة إذاعية بوسائلها الخاصة لاستخدامها في إذاعتها الخاصة. ويجوز لهذه التشريعات أن تصرح بحفظ هذه التسجيلات في محفوظات رسمية بالنظر لطابعها الاستثنائي كوثائق.

#### مادة ١١ (ثالثا)

(بعض الحقوق المتعلقة بالمصنفات الأدبية: (١) حق التلاوة العلنية ونقلها إلى الجمهور (٢) بالنسبة للترجمات)

(١) يتمتع مؤلفو المصنفات الأدبية بحق استثنائي في تصريح:  
(١) التلاوة العلنية لمصنفاتهم بما في ذلك التلاوة العلنية بجميع الوسائل أو الطرق.

(٢) نقل تلاوة مصنفاتهم إلى الجمهور بجميع الوسائل.  
(٣) يتمتع مؤلفو المصنفات الأدبية، طوال مدة سريان حقوقهم علي المصنف الأصلي، بنفس الحقوق فيما يتعلق بترجمة مصنفاتهم.

#### مادة ١٢

(حق تحويل المصنفات وتعديلها وإجراء أية تحويلات أخرى عليها)  
يتمتع مؤلفو المصنفات الأدبية أو الفنية بحق استثنائي في تصريح تحويل مصنفاتهم أو تعديلها أو إجراء أي تحويلات أخرى عليها.

## مادة ١٣

(إمكانية تحديد حق تسجيل المصنفات الموسيقية وأية كلمات مصاحبة لها: (١) التراخيص الإجبارية (٢) الإجراءات الإنتقالية (٤) مصادرة نسخ المصنفات المستوردة، المصنوعة دون تصريح من المؤلف)

(١) يجوز لكل دولة في الاتحاد أن تضع، فيما يخصها، تحفظات وشروط بشأن الحق الاستثنائي الممنوح لمؤلف مصنف موسيقي وللمؤلف أية كلمات يكون قد تم تسجيلها مع المصنف الموسيقي بتصريح من الأخير، وذلك في ترخيص التسجيل الصوتي لذلك المصنف الموسيقي مصحوبا بالكلمات إن وجدت. بيد أن كل مثل هذه التحفظات والشروط يقتصر تطبيقها على الدولة التي فرضتها، ولا يجوز أن تمس بأي حال بحق المؤلف في الحصول على مقابل عادل تحدده السلطة المختصة في حالة عدم الاتفاق عليه وديا.

(٢) تسجيلات المصنفات الموسيقية التي تم إنجازها في إحدى دول الاتحاد طبقا للمادة ١٣ (٣) من الوثيقتين لهذه الاتفاقية الموقعيتين في روما في ٢ يونيو ١٩٢٨ وفي بروكسل في ٢٦ يونيو ١٩٤٨، يمكن أن تكون محلا للنقل داخل تلك الدولة بغير موافقة مؤلف المصنف الموسيقي وذلك حتى نهاية مدة سنتين اعتبارا من التاريخ الذي تصبح فيه الدولة المذكورة مرتبطة بهذه الوثيقة.

(٣) التسجيلات التي تتم وفقا للفقرتين (١) و (٢) من هذه المادة والتي يتم استيرادها، بغير تصريح من الأطراف المعنية، في دولة تعتبرها تسجيلات مخالفة للقانون، تكون عرضة للمصادرة.

## مادة ١٤

(الحقوق السينمائية والحقوق المرتبطة بها: (١) التحوير والنسخ السينمائي، التوزيع، التمثيل والأداء العنفي والنقل السلبي إلى الجمهور

للمصنفات المحورة أو المنسوخة بهذا الشكل (٢) تحويل الإنتاج السينمائي  
(٣) عدم وجود تراخيص إجبارية)

(١) يتمتع مؤلفو المصنفات الأدبية أو الفنية بحق استثنائي في ترخيص:

(١) تحويل مصنفاتهم وعمل نسخ منها للإنتاج السينمائي، وتوزيع مثل  
هذه النسخ المحورة أو المنقولة.

(٢) التمثيل والأداء العلني والنقل السلبي للجمهور للمصنفات المحورة  
أو المنقولة بهذا الشكل.

(٢) تحويل الإنتاج السينمائي المأخوذ من مصنفات أدبية أو فنية، تحت  
أي شكل فني آخر، يظل خاضعا لتصريح مؤلفي المصنفات الأصلية، وذلك  
دون المساس بترخيص مؤلفي الإنتاج السينمائي.

(٣) لا تنطبق أحكام المادة ١٣ (١).

#### مادة ١٤ (ثانيا)

(أحكام خاصة تتعلق بالمصنفات السينمائية: (١) التشبيه بالمصنفات  
"الأصلية" (٢) أصحاب حق المؤلف، تحديد حقوق بعض المؤلفين  
المساهمين (٣) بعض المؤلفين المساهمين الآخرين)

(١) دون المساس بحق المؤلف لأي مصنف يكون قد تم تحويله أو نقله،  
يتمتع المصنف السينمائي بالحماية كمصنف أصلي. ويتمتع صاحب حق  
المؤلف لمصنف سينمائي بذات الحقوق التي يتمتع بها مؤلف مصنف أصلي،  
بما في ذلك الحقوق المشار إليها في المادة السابقة.

(٢) (أ) تحديد أصحاب حق المؤلف لمصنف سينمائي يختص به تشريع  
الدولة المطلوب توفير الحماية فيها.

(ب) ومع ذلك، ففي دول الاتحاد التي تقضي تشريعاتها تضمين أصحاب حق المؤلف في مصنف سينمائي المؤلفين الذين ساهموا في عمل المصنف، فإن مثل هؤلاء المؤلفين في حالة إذا ما تعهدوا بتقديم مثل هذه المساهمة، ليس لهم، ما لم يتفق علي خلاف ذلك أو علي نص خاص، أن يعترضوا علي عمل نسخ من المصنف السينمائي أو تداوله أو تمثيله أو أدائه علنا أو نقله سلكيا إلي الجمهور، أو إذاعته أو علي أي نقل آخر إلي الجمهور، أو تضمينه حاشية بالترجمة أو جعله ناطقا بلغة أخرى.

(ج) أمر البت فيما إذا كان يجب إفراغ التعهد المذكور أعلاه لأغراض تطبيق الفقرة الفرعية (ب) السابقة، في شكل عقد مكتوب أو محرر مكتوب له ذات النثر من عدمه، يختص به تشريع دولة الاتحاد التي يتخذها منتج المصنف السينمائي مقرا له أو محلا لإقامته المعتادة، ومع ذلك يختص تشريع دولة الاتحاد المطلوب توفير الحماية فيها بحق القضاء بما إذا كان التعهد المشار إليه يجب أن يكون عقدا مكتوبا أو محررا مكتوبا له ذات الأثر، ويجب علي الدول التي تقوم باستعمال هذا الحق أن تخطر المدير العام بذلك بموجب إعلان كتابي يقوم بإبلاغه في الحال إلي جميع دول الاتحاد الأخرى.

(د) يقصد بعبارة "ما لم يتفق علي خلاف ذلك أو علي نص خاص" أي شرط مقيد يمكن أن يخضع له التعهد المذكور.

(٣) لا تطبق أحكام الفقرة (٢) (ب) أعلاه علي مؤلفي السيناريو والحوار والمصنفات الموسيقية التي يتم تأليفها بغرض إنجاز مصنف سينمائي، ولا علي المخرج الرئيسي لهذا المصنف، هذا ما لم يقرر التشريع الوطني خلاف ذلك، ومع ذلك فعلي دول الاتحاد التي تخلق تشريعاتها من أحكام تقضي بتطبيق الفقرة (٢) (ب) المشار إليها علي المخرج المذكور، أن تخطر المدير العام بذلك بموجب إعلان كتابي يقوم بإبلاغه في الحال إلي جميع دول الاتحاد الأخرى.

## مادة ١٤ (ثالثا)

- (١) حق التتبع بشأن المصنفات الفنية والمخطوطات: (١) حق الانتفاع بعمليات إعادة البيع (٢) التشريعات المطبقة (٣) الإجراءات
- (١) فيما يتعلق بالمصنفات الفنية الأصلية والمخطوطات الأصلية لكتاب ومؤلفين موسيقيين، يتمتع المؤلف، أو من له صفة بعد وفاته من الأشخاص أو الهيئات وفقا للتشريع الوطني، بحق غير قابل للتصرف فيه، في تعلق مصلحتهم بعمليات بيع المصنف التالية لأول تنازل عن حق الاستغلال بحرية المؤلف.
- (٢) لا يمكن المطالبة بتوفير الحماية المنصوص عليها في الفقرة السابقة في أية دولة من دول الاتحاد إلا إذا كان تشريع الدولة التي ينتمي إليها المؤلف يقرر هذه الحماية وفي الحدود التي يسمح بها تشريع الدولة المطلوب توفير الحماية فيها.
- (٣) يختص التشريع الوطني بتحديد إجراءات التحصيل والمبالغ الواجبة.

## مادة ١٥

- (١) حق المطالبة بالحقوق المتمتعة بالحماية: (١) عند بيان اسم المؤلف أو عندما لا يدع الاسم المستعار مجالا لأي شك في تحديد شخصية المؤلف
- (٢) بالنسبة للمصنفات السينمائية (٣) بالنسبة للمصنفات التي لا تحمل اسم المؤلف أو التي تحمل اسما مستعارا (٤) بالنسبة لبعض المصنفات غير المنشورة والتي تكون شخصية مؤلفها مجهولة
- (١) لكي يعتبر أن لمؤلفي المصنفات الأدبية أو الفنية التي تحميها الاتفاقية الحالية هذه الصفة ويكون لهم بالتالي حق المثل أمام محاكم دول الاتحاد ومقاضاة من يمس بحقوقهم، يكفي أن يظهر اسم المؤلف علي المصنف بالطريقة المعتادة هذا ما لم يقر الدليل علي عكس ذلك، وتطبق هذه

الفقرة حتى إذا كان الاسم مستعاراً، متى كان الاسم المستعار الذي يتخذه المؤلف لا يدع مجالاً لأي شك في تحديد شخصيته.

(٢) يفترض أن الشخص الطبيعي أو الاعتباري الذي يظهر اسمه بالطريقة المعتادة علي مصنف سينمائي هو المنتج لهذا المصنف، هذا ما لم يّم الدليل علي عكس ذلك.

(٣) بالنسبة للمصنفات التي لا تحمل اسم المؤلف أو التي تحمل اسماً مستعاراً، غير تلك المشار إليها في الفقرة (١) أعلاه، يفترض أن الناشر الذي يظهر اسمه علي المصنف، وما لم يثبت عكس ذلك، بمثابة ممثل للمؤلف، وبهذه الصفة فإن له حق المحافظة علي حقوق المؤلف والدفاع عنها، ويوقف سريان حكم هذه الفقرة عندما يكشف المؤلف عن شخصيته ويثبت صفته.

(٤) (أ) بالنسبة للمصنفات غير المنشورة والتي تكون شخصية مؤلفها مجهولة، مع وجود كل ما يدعو إلي الاعتقاد بأنه من مواطني إحدى دول الاتحاد، فإن تشريع هذه الدولة يختص بحق تعيين السلطة المختصة التي تقوم بتمثيل المؤلف ويكون لها حق المحافظة علي حقوقه والدفاع عنها في دول الاتحاد.

(ب) علي دول الاتحاد التي تقوم بمثل هذا التعيين عملاً بالحكم المذكور أن تحظي المدير العام بذلك بمقتضى إعلان كتابي يتضمن كل البيانات الخاصة بالسلطة المختصة التي تم تعيينها بهذا الشكل، ويقوم المدير العام بإبلاغ ذلك في الحال إلي جميع دول الاتحاد الأخرى.

#### مادة ١٦

(المصنفات المزورة: (١) المصادرة (٢) المصادرة عند الاستيراد (٣) التشريعات المطبقة)

- (١) تكون جميع النسخ غير المشروعة لمصنف محلا للمصادرة في دول الاتحاد التي يتمتع فيها المصنف الأصلي بالحماية القانونية.
- (٢) تطبق أحكام الفقرة السابقة أيضا علي النسخ الواردة من دولة لا يتمتع فيها المصنف بالحماية أو تكون قد توقفت فيها حمايته.
- (٣) تجري المصادرة وفقا لتشريع كل دولة.

#### مادة ١٧

(إمكانية مراقبة تداول المصنفات وتمثيلها وعرضها)

لا يمكن لأحكام هذه الاتفاقية أن تمس بأي شكل بحق حكومة كل دولة من دول الاتحاد في أن تسمح أو تراقب أو تمنع، عن طريق التشريع أو إصدار اللوائح، تداول أو تمثيل أو عرض أي مصنف أو إنتاج تري السلطة المختصة ممارسة هذا الحق بالنسبة إليه.

#### مادة ١٨

(المصنفات الموجودة عند دخول الاتفاقية حيز التنفيذ: (١) يجوز حمايتها في حالة عدم انقضاء مدة الحماية في دولة المنشأ (٢) لا يجوز حمايتها في حالة انقضاء مدة الحماية في الدولة المطلوب توفير الحماية فيها (٣) تطبيق هذه المبادئ (٤) حالات خاصة)

(١) تسري هذه الاتفاقية علي كل المصنفات التي لا تكون، عند دخول هذه الاتفاقية حيز التنفيذ، قد سقطت بعد في الملك العام لدولة المنشأ، بانقضاء مدة الحماية.

(٢) ومع ذلك، إذا سقط أحد المصنفات في الملك العام في الدولة المطلوب توفير الحماية فيها، نتيجة لانقضاء مدة الحماية السابق منحها له، فإن هذا المصنف لا يتمتع فيها بالحماية من جديد.



(٣) يجري تطبيق هذا المبدأ وفقاً للأحكام التي تتضمنها الاتفاقيات الخاصة المعقودة أو التي قد تعقد لهذا الغرض فيما بين دول الاتحاد، وفي حالة عدم وجود مثل هذه الأحكام، تحدد الدول المعنية، كل فيما يخصها، الشروط الخاصة بتطبيق هذا المبدأ.

(٤) تنطبق الأحكام السابقة أيضاً في حالة انضمام دولة جديدة إلى الاتحاد وكذلك في الحالة التي تمتد فيها الحماية بالتطبيق للمادة ٧ أو بسبب التنازل عن التحفظات.

#### مادة ١٩

(تطبيق حماية أوسع من الحماية المترتبة على الاتفاقية)

لا تمنع أحكام هذه الاتفاقية من المطالبة بتطبيق حماية أوسع يكون قد قررها تشريع دولة من دول الاتحاد.

#### مادة ٢٠

(اتفاقات خاصة بين دول الاتحاد)

تحتفظ حكومات دول الاتحاد بالحق في عقد اتفاقات خاصة فيما بينها، ما دامت هذه الاتفاقات تخول حقوقاً تفوق تلك التي تمنحها هذه الاتفاقية، أو تتضمن نصوصاً لا تتعارض مع هذه الاتفاقية، وتبقى أحكام الاتفاقات القائمة سارية متى كانت مطابقة للشروط السابق ذكرها.

#### مادة ٢١

(أحكام خاصة تتعلق بالبلدان النامية: (١) الرجوع إلى الملحق (٢) الملحق جزء لا يتجزأ من الوثيقة)

(١) يتضمن الملحق أحكاماً خاصة تتعلق بالدول النامية.

(٢) مع مراعاة أحكام المادة ٢٨ (١) (ب)، بشكل الملحق جزءاً لا يتجزأ من هذه الوثيقة.

## مادة ٢٢

- (الجمعية: (١) الإنشاء والتشكيل (٢) المهام (٣) النصاب القانوني، التصويت، المراقبون (٤) الدعوة للاجتماع (٥) النظام الداخلي)
- (١) (أ) يكون للاتحاد جمعية تتكون من دول الاتحاد الملزمة بالمواد من ٢٢ إلى ٢٦.
- (ب) تمثل حكومة كل دولة بمندوب واحد يمكن أن يعاونه مناوون ومستشارون وخبراء.
- (ج) تتحمل نفقات كل وفد الحكومة التي عينته.
- (٢) (أ) تقوم الجمعية بما يلي:
- (١) تعالج جمعية المسائل الخاصة بالمحافظة علي الاتحاد وتنميته وتنفيذ هذه الاتفاقية.
- (٢) تزود المكتب الدولي للملكية الفكرية (ويدعي فيما بعد "المكتب الدولي") المشار إليه في اتفاقية إنشاء المنظمة العالمية للملكية الفكرية (وتدعي فيما بعد "المنظمة") بالتوجيهات الخاصة بالإعداد لمؤتمرات التعديل، مع مراعاة ملاحظات دول الاتحاد غير الملزمة بالمواد من ٢٢ إلى ٢٦.
- (٣) تنظر في تقارير وأنشطة مدير عام المنظمة الخاصة بالاتحاد وتعتمدها، وتزوده بجميع التوجيهات اللازمة بخصوص الموضوعات التي تدخل في اختصاص الاتحاد.
- (٤) تنتخب أعضاء اللجنة التنفيذية للجمعية.

(٥) تُنظر في تقارير وأنشطة لجنّتها التنفيذيّة وتُعتمدها وتزودها بالتوجيهات.

(٦) تُحدد برنامج الاتحاد وتقر ميزانية فترة السنتين الخاصّة به وتعتمد حساباته الختامية.

(٧) تقر اللاتحة الماليّة للاتحاد.

(٨) تنشئ ما تراه ملائماً من لجان خبراء وجماعات عمل لتحقيق أغراض الاتحاد.

(٩) تُحدد من يسمح لهم بحضور اجتماعاتهم كمراقبين من الدول غير الأعضاء في الاتحاد ومن المنظمات الدوليّة الحكوميّة وغير الحكوميّة.

(١٠) تقر التعديلات الخاصّة بالمواد من ٢٢ إلى ٢٦.

(١١) تتخذ أي إجراء آخر ملائم بهدف إلى تحقيق أغراض الاتحاد.

(١٢) تباشر أية مهام أخرى تدخل في نطاق هذه الاتفاقية.

(١٣) تمارس الحقوق الممنوحة لها بموجب اتفاقية إنشاء المنظمة شريطة قبولها لهذه الحقوق.

(ب) تتخذ الجمعية قراراتها فيما يتعلق بالموضوعات التي تهم أيضاً لتحادات أخرى تديرها المنظمة بعد الإطلاع على رأي لجنة التنسيق التابعة للمنظمة.

(٣) (أ) يكون لكل دولة عضو في الجمعية صوت واحد.

(ب) يتكون النصاب القانوني من نصف عدد الدول الأعضاء في الجمعية.

(ج) بغض النظر عن أحكام الفقرة الفرعية (ب)، للجمعية أن تتخذ قراراتها إذا كان عدد الدول الممثّلة في أية دورة يقل عن النصف ولكن يساوي ثلث الدول الأعضاء في الجمعية أو يزيد عليه، ومع ذلك فإن قرارات

دورة الجمعية، بخلاف تلك المتعلقة بإجراءاتها، لا تكون نافذة إلا إذا توفرت الشروط التالية. يبلغ المكتب الدولي القرارات المذكورة إلى الدول الأعضاء في الجمعية التي لم تكن ممثلة، ويدعوها إلى الإدلاء بتصويتها أو امتناعها كتابة خلال مدة ثلاثة شهور من تاريخ ذلك الإبلاغ، فإذا ما كان عدد الدول التي أدلت بتصويتها أو امتناعها عند انقضاء تلك المدة يساوي علي الأقل العدد الذي كان مطلوباً لاستكمال النصاب القانوني في الدورة ذاتها تكون تلك القرارات نافذة متى كانت الأغلبية المطلوبة ما زالت قائمة في نفس الوقت.

(د) مع مراعاة أحكام المادة ٢٦ (٢) تتخذ قرارات الجمعية بأغلبية ثلثي الأصوات التي اشتركت في الاقتراع.

(هـ) لا يعتبر الامتناع بمثابة تصويت.

(و) لا يمثل المندوب إلا دولة واحدة فقط ولا يصوت إلا باسمها.

(ز) تشارك دول الاتحاد غير الأعضاء في الجمعية في اجتماعاتها كمرأقين.

(٤) (أ) تجتمع الجمعية في دورة عادية مرة كل سنتين بدعوة من المدير العام، ويكون اجتماعها، فيما عدا الحالات الاستثنائية، أثناء نفس الفترة وفي نفس المكان الذين تجتمع فيهما الجمعية العامة للمنظمة.

(ب) تجتمع الجمعية في دورة غير عادية بدعوة من المدير العام بناء علي طلب اللجنة التنفيذية أو علي طلب ربع عدد الدول الأعضاء في الجمعية.

(٥) تضع الجمعية النظام الداخلي الخاص بها.

#### مادة ٢٣

(اللجنة التنفيذية: (١) الإنشاء (٢) التشكيل (٣) عدد الأعضاء (٤) التوزيع الجغرافي، اتفاقات خاصة (٥) مدة التفويض، حدود الأهلية لإعادة

الانتخاب، القواعد المتبعة بشأن الانتخاب (٦) المهام (٧) الدعوة للاجتماع  
(٨) النصاب القانوني، التصويت (٩) المراقبون (١٠) النظام الداخلي

(١) يكون للجمعية لجنة تنفيذية.

(٢) (أ) تكون اللجنة التنفيذية من الدول التي تنتخبها الجمعية من بين  
الدول الأعضاء فيها، وعلاوة على ذلك يكون للدولة التي يقع على إقليمها  
مقر المنظمة، بحكم وضعها، مقعد في اللجنة وذلك مع مراعاة أحكام المادة  
٢٥ (٧) (ب).

(ب) تمثل حكومة كل دولة عضو في اللجنة التنفيذية بمندوب واحد يمكن  
أن يعاونه منابرون ومستشارون وخبراء.

(ج) تتحمل نفقات كل وفد الحكومة التي عينته.

(٣) يكون عدد الدول الأعضاء في اللجنة التنفيذية مساويا لربع عدد  
الدول الأعضاء في الجمعية، وعند تحديد عدد المقاعد التي يتعين شغلها يهمل  
الباقى بعد القسمة على أربعة.

(٤) تراعى الجمعية عند انتخاب أعضاء اللجنة التنفيذية توزيعا جغرافيا  
عادلا وضرورة أن تكون الدول الأطراف في الاتفاقات الخاصة التي يمكن  
أن تعقد في إطار الاتحاد ضمن الدول التي تتكون منها اللجنة التنفيذية.

(٥) (أ) يتولى أعضاء اللجنة التنفيذية مهام عملهم ابتداء من ختام دورة  
الجمعية التي تم فيها انتخابهم حتى ختام الدورة العادية التالية للجمعية.

(ب) يمكن إعادة انتخاب أعضاء اللجنة التنفيذية ولكن بحد أقصى لا يزيد  
على ثلاثي عندهم.

(ج) تضع الجمعية القواعد التفصيلية الخاصة بانتخاب وإعادة الانتخاب  
المحتمل لأعضاء اللجنة التنفيذية.

(٦) (أ) تقوم اللجنة التنفيذية بما يلي:

- (١) تعد مشروع جدول أعمال الجمعية.
- (٢) تعرض علي الجمعية مقترحات متعلقة بمشروع البرنامج ومشروع ميزانية فترة السنتين الخاصة بالاتحاد والمعدة من قبل المدير العام.
- (٣) (تُحذف).
- (٤) تعرض علي الجمعية، مع التعليقات الملائمة، التقارير الدورية للمدير العام والتقارير السنوية الخاصة بمراجعة الحسابات.
- (٥) تتخذ كافة الإجراءات اللازمة لضمان قيام المدير العام بتنفيذ برنامج الاتحاد طبقاً لقرارات الجمعية مع مراعاة الظروف التي قد تطرأ فيما بين دورتين عاديتين للجمعية.
- (٦) تباشر أية مهام أخرى تعهد إليها في نطاق هذه الاتفاقية.
- (ب) تتخذ اللجنة التنفيذية قراراتها فيما يتعلق بالموضوعات التي تهم أيضاً اتحادات أخرى تديرها المنظمة بعد الإطلاع علي رأي لجنة التنسيق التابعة للمنظمة.
- (٧) (أ) تجتمع اللجنة التنفيذية في دورة عادية مرة كل سنة بدعوى من المدير العام، ويتم الاجتماع أثناء نفس الفترة وفي نفس المكان اللذين تجتمع فيهما لجنة التنسيق التابعة للمنظمة وذلك بقدر الإمكان.
- (ب) تجتمع اللجنة التنفيذية في دورة غير عادية بدعوى من المدير العام إما بمبادرة منه أو بناء علي طلب رئيسها أو ربع أعضائها.
- (٨) (أ) يكون لكل دولة عضو في اللجنة التنفيذية صوت واحد.
- (ب) يتكون النصاب القانوني من نصف عدد الدول الأعضاء في اللجنة التنفيذية.
- (ج) تتخذ القرارات بالأغلبية البسيطة للأصوات التي اشتركت في الاقتراع.
- (د) لا يعتبر الامتناع بمثابة تصويت.

(هـ) لا يمثل المندوب إلا دولة واحدة فقط ولا يصوت إلا باسمها.  
(٩) لدول الاتحاد غير الأعضاء في اللجنة التنفيذية أن تحضر اجتماعاتها كمراقبين.

(١٠) تضع اللجنة التنفيذية النظام الداخلي الخاص بها.

#### مادة ٢٤

- (المكتب الدولي: (١) مهامه بوجه عام، المدير العام (٢) معطومات عامة (٣) مجلة دورية (٤) تزويد الدول بالمعلومات (٥) دراسات وخدمات (٦) الاشتراك في الاجتماعات (٧) مؤتمرات التعديل (٨) مهام أخرى
- (١) (أ) يمارس المكتب الدولي المهام الإدارية الخاصة بالاتحاد، ويعتبر المكتب الدولي امتدادا لمكتب الاتحاد المتحد مع مكتب الاتحاد الذي أنشأته الاتفاقية الدولية لحماية الملكية الصناعية.
- (ب) يقوم المكتب الدولي، بصفة خاصة، بأعمال السكرتارية لمختلف أجهزة الاتحاد.
- (ج) المدير العام للمنظمة هو الرئيس التنفيذي للاتحاد وهو الذي يمثلها.
- (٢) يجمع المكتب الدولي المعلومات الخاصة بحماية حق المؤلف وينشرها، وتقوم كل دولة من دول الاتحاد بتزويد المكتب الدولي، في أقرب وقت ممكن، بجميع القوانين الجديدة والنصوص الرسمية المتعلقة بحماية حق المؤلف.
- (٣) يصدر المكتب الدولي مجلة شهرية.
- (٤) يزود المكتب الدولي كل دولة في الاتحاد، بناء على طلبها، بمعلومات عن المسائل المتعلقة بحماية حق المؤلف.
- (٥) يجري المكتب الدولي دراسات ويقدم خدمات تهدف إلى تيسير حماية حق المؤلف.

(٦) يشترك المدير العام، وأي عضو يكلفه من موظفي المكتب الدولي، في كافة اجتماعات الجمعية واللجنة التنفيذية وأية لجنة خبراء أخرى أو جماعة عمل، دون أن يكون لهم حق التصويت، ويكون المدير العام، أو أي عضو يكلفه من موظفي المكتب الدولي، سكرتيراً لهذه الأجهزة بحكم منصبه.

(٧) (أ) يقوم المكتب الدولي، وفقاً لتوجيهات الجمعية وبالتعاون مع اللجنة التنفيذية، بإعداد مؤتمرات التعديل الخاصة بأحكام الاتفاقية فيما عدا المواد من ٢٢ إلى ٢٦.

(ب) للمكتب الدولي أن يتشاور مع المنظمات الدولية الحكومية وغير الحكومية بشأن الإعداد لمؤتمرات التعديل.

(ج) يشترك المدير العام والأشخاص الذين يعينهم في مناقشات هذه المؤتمرات دون أن يكون لهم حق التصويت.

(٨) ينفذ المكتب الدولي أية مهام أخرى تعهد إليه.

#### مادة ٢٥

الشنون المالية: (١) الميزانية (٢) التنسيق مع الاتحادات الأخرى (٣) المصادر المالية (٤) الحصص، إمكانية تجديد الميزانية (٥) الرسوم والمبالغ المستحقة (٦) صندوق رأس المال العامل (٧) قروض مقدمة من طرف الحكومة المضيفة.

(١) (أ) يكون للاتحاد ميزانية.

(ب) تشمل ميزانية الاتحاد الإيرادات والنفقات الخاصة بالاتحاد ومساهمته في ميزانية النفقات المشتركة بين الاتحادات. وكذلك إذا اقتضى الأمر، المبلغ الموضوع تحت تصرف ميزانية مؤتمر المنظمة.



(ج) تعتبر نفقات مشتركة بين الاتحادات النفقات التي لا تخص الاتحاد وحده، بل تخص كذلك واحدا أو أكثر من الاتحادات الأخرى التي تديرها المنظمة، ويكون نصيب الاتحاد في هذه النفقات المشتركة بنسبة المصلحة التي تعود عليه منها.

(٢) توضع ميزانية الاتحاد بعد اعتبار مقتضيات التنسيق مع ميزانيات الاتحادات الأخرى التي تديرها المنظمة.

(٣) تمول ميزانية الاتحاد من المصادر التالية:

(١) حصص دول الاتحاد.

(٢) الرسوم والمبالغ المستحقة عن الخدمات التي يؤديها المكتب الدولي مما يخص الاتحاد.

(٣) حصيلة بيع مطبوعات المكتب الدولي الخاصة بالاتحاد والحقوق المتصلة بهذه المطبوعات.

(٤) الهبات والوصايا والاعانات.

(٥) الإيجارات والفوائد والإيرادات المتنوعة الأخرى.

(٤) (أ) لتحديد حصة كل دولة من دول الاتحاد في الميزانية، تنتمي تلك الدولة إلى فئة وتقوم بدفع حصصها السنوية على أساس عدد من الوحدات محددة كما يلي:

٢٥	فئة ١
٣٠	فئة ٢
١٥	فئة ٣
١٠	فئة ٤
٥	فئة ٥

(ب) تبيين كل دولة الفئة التي ترغب في الانتماء إليها عند إيداعها وثيقة التصديق أو الانضمام الخاصة بها، ما لم يكن قد سبق لها بيان ذلك. ويمكن لسلك الدولة أن تغير الفئة التي تنتمي إليها، فإذا ما اختارت فئة أدنى فعليها أن تعلن ذلك للجمعية في إحدى دوراتها العادية. ويصبح أى تغيير من هذا القبيل سارى المفعول من بداية السنة التالية للدورة المذكورة.

(ج) تكون الحصص السنوية لكل دولة مبلغا تبلغ نسبته إلى المبلغ الإجمالي للاشتراكات السنوية في ميزانية الاتحاد، ما يعادل نسبة عدد وحدات تلك الدولة إلى إجمالي الوحدات الخاصة بجميع الدول المساهمة.

(د) تستحق الحصص في أول يناير من كل سنة.

(هـ) لا يجوز للدولة التي تتأخر في دفع حصصها أن تباشر حقها في التصويت في أى من أجهزة الاتحاد الذى تتمتع بعضويته إذا كان مقدار ديونها المتأخرة يعادل مبلغ الحصص المستحقة عليها عن السنتين السابقتين بالكامل أو يزيد عليه. ومع ذلك يجوز لأى من أجهزة الاتحاد أن يسمح لتلك الدولة بالاستمرار في مباشرة حقها في التصويت في مثل هذا الجهاز مادام كان مقتنعا بأن التأخير في الدفع ناتج عن ظروف استثنائية لا يمكن تجنبها.

(و) إذا لم يتم إقرار الميزانية قبل بداية سنة مالية جديدة يستمر العمل بميزانية السنة المنتهية وذلك طبقا لما تقضي به اللائحة المالية.

(٥) يحدد المدير العام مقدار الرسوم والمبالغ المستحقة عن الخدمات التي يؤديها المكتب الدولي لمصلحة الاتحاد وتقدم تقارير عنها إلى الجمعية واللجنة التنفيذية.

(٦) (أ) يكون للاتحاد صندوق لرأس المال العامل يتكون من مبلغ يدفع لمرة واحدة من قبل كل دولة من دول الاتحاد وتقرر الجمعية زيادة رأس المال إذا أصبح غير كاف.

(ب) يكون مقدار الدفعة الأولى الخاصة بكل دولة في رأس المال السالف الذكر أو اشتراكها في أية زيادة له عبارة عن نسبة من حصة تلك الدولة عن السنة التي تحدد فيها رأس المال أو تقررت فيها زيادته.

(ج) تحدد الجمعية نسبة الدفعة وشروط دفعها بناء على اقتراح المدير العام وبعد الاطلاع على رأى لجنة التنسيق التابعة للمنظمة.

(٧) (أ) ينص اتفاق المقر المبرم مع الدولة التي يكون مقر المنظمة على إقليمها على أنه عند ما يكون رأس المال العامل غير كاف تقوم تلك الدولة بمنح قروض. ويكون مقدار هذه القروض وشروط منحها موضوعا للاتفاقات منفصلة في كل حالة بين تلك الدولة والمنظمة. وتتمتع تلك الدولة بحكم وضعها بمقعد في اللجنة التنفيذية مادامت تظل ملتزمة بتقديم قروض.

(ب) يحق لكل من الدولة المشار إليها في الفقرة الفرعية (أ) والمنظمة أن تنهي الالتزام بمنح قروض بموجب إخطار كتابي. ويسرى مفعول الإنهاء بعد ثلاث سنوات من نهاية السنة التي تم فيها الإخطار عنه.

(٨) تتم مراجعة الحسابات. وفقا لما تنص عليه اللائحة المالية. من قبل دولة أو أكثر من دول الاتحاد أو منق بل مراقبي حسابات من الخارج تعبئهم الجمعية بعد أخذ موافقتهم.

## مادة ٢٦

التعديلات: (أ) أحكام يجوز تعديلها من قبل الجمعية. اقتراحات (٢)  
الإقرار (٣) بدء النفاذ.

(١) لأية دولة عضو في الجمعية وللجنة التنفيذية وكذلك للمدير العام التقدم باقتراحات لتعديل المواد ٢٢، ٢٣، ٢٤، ٢٥ بالإضافة للمادة الحالية. ويقوم المدير العام بإبلاغ تلك الاقتراحات إلى الدول الأعضاء في الجمعية قبل نظرها من قبل الجمعية بسنة أشهر على الأقل.

(٢) تستولى الجمعية إقرار التعديلات الخاصة بالمواد المشار إليها في الفقرة (١). ويتطلب هذا الإقرار ثلاثة أرباع عدد الأصوات التي اشتركت في الاقتراح. ومع ذلك فإن أي تعديل للمادة ٢٢ وللفقرة الحالية يتطلب أربعة أخماس عدد الأصوات التي اشتركت في الاقتراح.

(٣) يبدأ نفاذ أي تعديل للمواد المشار إليها في الفقرة (١) بعد شهر مع تسلم المدير العام إخطارات كتابية بموافقة ثلاثة أرباع عدد الدول الأعضاء في الجمعية، وذلك في وقت إقرارها للتعديل، وعلى أن تكون تلك الموافقات قد تمت وفقاً للإجراءات الدستورية الخاصة بهذه الدول. وتلزم أية تعديلات للمواد المذكورة، يكون قد تم إقرارها بهذا الشكل، جميع الدول الأعضاء في الجمعية عند بدء نفاذ التعديل أو التي تصبح أعضاء فيها في تاريخ لاحق، ومع هذا فإن أي تعديل يزيد من الالتزامات المالية للدول الأعضاء في الاتحاد لا يلزم إلا تلك الدول التي قامت بالإخطار عن موافقتها على التعديل المذكور.

## مادة ٢٧

تعديل الاتفاقية : (١) الغرض (٢) المؤتمرات (٣) الإقرار

(١) تكون هذه الاتفاقية محلاً للتعديل بغرض إدخال تغييرات تهدف إلى تحسين نظام الاتحاد.

(٢) ولهذا الغرض تعقد مؤتمرات في دول الاتحاد على التوالي بين مندوبي هذه الدول.

(٣) مع مراعاة أحكام المادة ٢٦ التي تنطبق على تعديل المواد من ٢٢ إلى ٢٦، فإن أى تعديل للوثيقة الحالية بما فى ذلك الملحق، يتطلب إجماع الأصوات التى اشتركت فى الاقتراح.

#### مادة ٢٨

قبول الوثيقة ونفاذها بالنسبة لدول الاتحاد: (١) التصديق، الانضمام، إماتية استبعاد بعض الأحكام، سحب الاستبعاد. (٢) بدء نفاذ المواد من ١ إلى ٢١ وكذلك الملحق (٣) بدء نفاذ المواد من ٢٢ إلى ٢٨.

(١) (أ) يجوز لكل دولة من دول الاتحاد الموقعة على هذه الوثيقة أن تصدق عليها. وإذا لم تكن قد وقعت فبوسعها الانضمام إليها، وتودع وثائق التصديق أو الانضمام لدى المدير العام.

(ب) يجوز لكل دولة من دول الاتحاد أن تعلن فى وثيقة التصديق أو الانضمام أن تصديقها أو انضمامها لا يسرى على المواد من ١ إلى ٢١ ولا على الملحق، ومع هذا، إذا كانت تلك الدولة قد قامت فعلاً بإعلان طبقاً للمادة السادسة (١) من الملحق، فليس فى وسعها الإعلان فى الوثيقة المذكورة إلا بأن تصديقها أو انضمامها لا يسرى على المواد من ١ إلى ٢٠.

(ج) يمكن لكل دولة من دول الاتحاد تكون طبقاً للفقرة الفرعية (ب)، قد استبعدت من آثار تصديقها أو انضمامها الأحكام المنصوص عليها فى الفقرة المذكورة أن تعلن فى أى وقت لاحق بأن آثار تصديقها أو انضمامها تمتد إلى هذه الأحكام. ويودع مثل هذا الإعلان لدى المدير العام.

(٢) (أ) يبدأ نفاذ المواد من ١ إلى ٢١ والملحق بعد ثلاثة شهور من توافر الشرطين التاليين:

(١) تصديق خمس دول على الأقل من دول الاتحاد على هذه الوثيقة أو انضمامها إليها دون القيام بالإعلان المنصوص عليه فى الفقرة (١) (ب).

(٢) أن تصبح كل فرنسا وأسبانيا والمملكة المتحدة والولايات المتحدة الأمريكية ملتزمة بالاتفاقية العالمية لحقوق المؤلف كما عدلت في باريس في ٢٤ يوليو ١٩٧١.

(ب) يسرى النفاذ المنصوص عليه في الفقرة الفرعية السابقة (أ) على دول الاتحاد السوفيتي أودعت قبل موعد السريان المذكور بثلاثة شهور وثائق تصديق أو انضمام خالصة من الإعلان المشار إليه في الفقرة (١) (ب).

(ج) يبدأ نفاذ المواد من ١ إلى ٢١ والملحق، بالنسبة لكل دولة من دول الاتحاد لا تنطبق عليها الفقرة الفرعية (١) (ب)، بعد ثلاثة شهور من التاريخ الذي يتولى فيه المدير العام إبلاغ الإخطار عن إيداع وثيقة التصديق أو الانضمام المعنية، ما لم تحدد الوثيقة المودعة تاريخاً لاحقاً، ففي هذه الحالة الأخيرة يبدأ نفاذ المواد من ١ إلى ٢١ والملحق بالنسبة لتلك الدولة من التاريخ الذي حددته في تلك الوثيقة.

(د) لا تؤثر أحكام الفقرات الفرعية من (أ) إلى (ج) على تطبيق المادة السادسة من الملحق.

(٤) يبدأ نفاذ المواد من ٢٢ إلى ٣٨، بالنسبة لكل دولة في الاتحاد تصديق على هذه الوثيقة أو تنضم إليها مع القيام بالإعلان المنصوص عليه في الفقرة (١) (ب) أو بدونه، بعد ثلاثة شهور من التاريخ الذي يتولى فيه المدير العام إبلاغ الإخطار عن إيداع وثيقة التصديق أو الانضمام المعنية، ما لم تحدد الوثيقة المودعة تاريخاً لاحقاً، ففي هذه الحالة الأخيرة يبدأ نفاذ المواد من ٢٢ إلى ٨٣ بالنسبة لتلك الدولة من التاريخ الذي حددته في تلك الوثيقة.

#### مادة ٢٩

قبول الوثيقة ونفاذها بالنسبة للدول خارج الاتحاد: الانضمام (٢) النفاذ.

(١) لكل دولة خارج الاتحاد أن تتضمن إلى هذه الوثيقة وأن تصبح بمقتضى ذلك طرفاً فى الاتفاقية الحالية وعضواً فى الاتحاد، وتودع وثائق الانضمام لدى المدير العام.

(٢) (أ) مع مراعاة الفقرة الفرعية (ب). يبدأ نفاذ هذه الاتفاقية بالنسبة لكل دولة خارج الاتحاد بعد ثلاثة شهور من التاريخ الذى يتولى فيه المدير العام إبلاغ الإخطار عن إيداع وثيقة انضمامها، وذلك ما لم تكن الوثيقة المودعة قد حددت تاريخاً لاحقاً، وفى هذه الحالة الأخيرة يبدأ نفاذ هذه الاتفاقية بالنسبة لتلك الدولة من التاريخ الذى حددته فى تلك الوثيقة.

(ب) إذا كان بدء النفاذ طبقاً للفقرة الفرعية (أ) يسبق بدء نفاذ المواد من ١ إلى ٢١ والملحق طبقاً للمادة ٢٨ (٢)(أ)، فإن الدولة المذكورة تكون ملتزمة خلال هذه الفترة بالمواد من ١ إلى ٢٠ من وثيقة بروكسل للاتفاقية الحالية بدلاً من المواد من ١ إلى ٢١ والملحق.

#### مادة ٢٩ (ثانياً)

آثار قبول الوثيقة من أجل تطبيق المادة ١٤ (٢) من اتفاقية إنشاء المنظمة العالمية للملكية الفكرية (ويبو).

التصديق على هذه الوثيقة أو الانضمام إليها من قبل كل دولة غير ملتزمة بالمواد من ٢٢ إلى ٣٨ من وثيقة استكهولم للاتفاقية الحالية يقوم مقام التصديق على وثيقة استكهولم المذكورة أو الانضمام إليها مع التحديد المنصوص عليه فى مادتها ٢٨ (١)(ب)(١)، وذلك من أجل إمكان تطبيق المادة ١٤ (٢) من اتفاقية إنشاء المنظمة لا غير.

#### مادة ٣٠

التحفظات: (١) حدود إمكانية إبداء التحفظات (٢) تحفظات سابقة، تحفظ بشأن حق الترجمة، سحب التحفظ.

(١) يترتب تلقائياً على التصديق أو الانضمام قبول جميع أحكام هذه الوثيقة والتمتع بجميع مزاياها، وذلك مع مراعاة ما هو مسموح به من استثناءات في الفقرة (٢) من هذه المادة والمادة ٢٨ (١)(ب) والمادة ٣٣ (٢) وكذلك الملحق.

(٢) (أ) مع مراعاة المادة الخامسة (٢) من الملحق، لكل دولة من دول الاتحاد تصديق على هذه الوثيقة أو تنضم إليها أن تتمتع بمزايا التحفظات التي أبدتها في السابق، شريطة أن تقوم بإعلان في هذا الخصوص حين إيداع وثقتها الخاصة بالتصديق أو الانضمام.

(ب) لكل دولة خارج الاتحاد أن تعلن، عند انضمامها إلى هذه الاتفاقية ومع مراعاة المادة الخامسة (٢) من الملحق، أنها تتوى أن تطبق، بصفة مؤقتة على الأقل، أحكام المادة ٥ من اتفاقية الاتحاد لعام ١٨٨٦، والمكملة في باريس عام ١٨٦٩ بدلاً من المادة ٨ من هذه الوثيقة المتعلقة بحق الترجمة، على أن يكون معلوماً أن هذه الأحكام لا تشمل إلا الترجمة إلى لغة عامة التداول في تلك الدولة. ومع مراعاة المادة الأولى (٦)(ب) من الملحق، فلكل دولة الحق في أن تطبق، بالنسبة إلى حق ترجمة مصنفات تكون دولة منشئها دولة تطبق مثل هذا التحفظ، حماية مماثلة لتلك التي تمنحها الدولة الأخيرة.

(ج) لكل دولة أن تسحب، في أي وقت، مثل هذه التحفظات بإخطار يوجه للمدير العام.

### مادة ٣١

قابلية التطبيق على بعض الأقاليم: (١) الإعلان (٢) سحب الإعلان (٣) تاريخ بدء نفاذ الإعلان أو سحبه (٤) عدم جواز التفسير الذي يتضمن قبول الوضع الراهن.

(١) لكل دولة أن تعلن في وثيقة تصديقها أو انضمامها أو أن تخطر المدير العام كتابة، في أي وقت لاحق، عن سريان هذه الوثيقة على كل أو



جزء من الأقاليم المحددة في التصريح أو الإخطار التي تكون الدولة مسؤولة عن علاقاتها الخارجية.

(٢) لكل دولة تكون قد أصدرت ذلك الإعلان أو أرسلت ذلك الإخطار أن تخطر المدير العام، في أي وقت، باتفاق سريان هذه الاتفاقية على تلك الأقاليم أو جزء منها.

(٣) (أ) يكون كل إعلان صدر بمقتضى الفقرة (١) نافذا اعتباراً من نفس التاريخ الخاص بالتصديق أو الانضمام الذي أدرج هذا الإعلان في وثيقته، ويكون كل إخطار أرسل بمقتضى تلك الفقرة نافذا بعد ثلاثة شهور من قيام المدير العام بالإخطار عنه.

(ب) يكون كل إخطار صدر بمقتضى الفقرة (٢) نافذا بعد إثني عشر شهراً من تسلم المدير العام له.

(٤) يجب ألا تفسر هذه المادة بأنها تعني الاعتراف أو الموافقة الضمنية من جانب أية دولة من دول الاتحاد بالوضع الراهن المتعلق بأى إقليم تنطبق عليه هذه الاتفاقية من قبل دولة أخرى من دول الاتحاد بمقتضى تصريح تم طبقاً للفقرة (١).

## مادة ٢٢

قابلية تطبيق هذه الوثيقة والوثائق السابقة: (١) بين دول الاتحاد (٢) بين دولة أصبحت عضواً في الاتحاد وبقيّة الدول الأعضاء في الاتحاد (٣) قابلية تطبيق الملحق في إطار بعض العلاقات.

(١) تحل هذه الوثيقة بالنسبة للعلاقة بين دول الاتحاد، وفي حدود سريانها، محل اتفاقية برن المؤرخة ٩ سبتمبر ١٨٨٦ ووثائق التعديل اللاحقة، أما الوثائق التي كانت نافذة المفعول في الماضي فتظل سارية بأكملها أو في الحدود التي لا تحل فيها محلها هذه الوثيقة بمقتضى الجملة

السابقة، وذلك بالنسبة للعلاقات مع دول الاتحاد التي لم تصدق على هذه الوثيقة أو لم تتضمن إليها.

(٢) مع مراعاة أحكام الفقرة (٣)، تقوم الدول التي هي خارج الاتحاد والتي تصبح طرفاً في هذه الوثيقة بتطبيقها بالنسبة لكل دولة من دول الاتحاد لا تكون ملتزمة بهذه الوثيقة أو تكون ملتزمة بها ولكنها قد قامت بالإعلان المنصوص عليه في المادة ٢٨(١)(ب). وتقر تلك الدول أن لدولة الاتحاد المذكورة في علاقاتها معها:

(١) أن تطبق أحكام أحدث وثيقة تلتزم بها.

(٢) أن يكون لها الحق في تطبيق الحماية بالمستوى المنصوص عليه في هذه الوثيقة، وذلك مع مراعاة أحكام المادة الأولى (٦) من الملحق.

(٣) لكل دولة طالبت بالتمتع بالحقوق المنصوص عليها في الملحق أن تطبق أحكام الملحق الخاصة بالحق أو الحقوق التي طالبت بالتمتع بها وذلك في علاقاتها مع أية دولة أخرى من دول الاتحاد غير الملتزمة بهذه الوثيقة شريطة أن تكون هذه الدولة الأخيرة قد قبلت تطبيق الأحكام المنكورة.

## مادة ٢٢

المنازعات: (١) اختصاص محكمة العدل الدولية (٢) التحفظ فيما يتعلق بهذا الاختصاص (٣) سحب التحفظ.

(١) كل نزاع بين اثنين أو أكثر من دول الاتحاد بشأن تفسير أو تطبيق هذه الاتفاقية والذي لا تتم تسويته بالمفاوضات يمكن لأي من الدول المعنية عرضة أمام محكمة العدل الدولية بعريضة تقدم وفقاً لنظام المحكمة، وذلك ما لم تتفق الدول المعنية على طريقة أخرى للتسوية، وتقوم الدول

التي تعرض النزاع أمام المحكمة بإخطار المكتب الدولي الذي يتولى إحاطة دول الاتحاد الأخرى علما بالموضوع.

(٢) لكل دولة أن تعلن، عند توقيعها للوثيقة الحالية أو إيداعها لوثيقة تصديقها أو انضمامها، أنها لا تعتبر نفسها ملتزمة بأحكام الفقرة (١). ولا تسرى أحكام الفقرة (١) فيما يختص بكل نزاع بين تلك الدولة وأية دولة أخرى من دول الاتحاد.

(٣) لكل دولة أصدرت إعلانا طبقا للفقرة (٢) أن تسحب تصريحها، في أي وقت، بإخطار يوجه للمدير العام.

#### مادة ٢٤

انتهاء مفعول بعض الأحكام السابقة: (١) بالنسبة لوثائق سابقة (٢) بالنسبة للبروتوكول الملحق بوثيقة استكهولم.

(١) مع مراعاة أحكام المادة ٢٩ (ثانيا)، لا يجوز لأية دولة أن تتضمن إلى وثائق سابقة لهذه الاتفاقية أو تصدق عليها، وذلك بعد بدء نفاذ المواد من ١ إلى ٢١ والملحق.

(٢) لا يجوز لأية دولة أن تصدر نصريحا طبقا للمادة ٥ من البروتوكول الخاص بالدول الناحية الملحق بوثيقة استكهولم، وذلك بعد بدء نفاذ المواد من ١ إلى ٢١ والملحق.

#### مادة ٢٥

مدة الاتفاقية، الانسحاب: (١) مدة غير محدودة (٢) إمكانية الانسحاب (٣) تاريخ بدء نفاذ الانسحاب (٤) مهلة الانسحاب. (١) تظل هذه الاتفاقية نافذة لمدة غير محددة.

(٢) لكل دولة أن تتسحب من هذه الوثيقة بإخطار يوجه إلى المدير العام ويشكل هذا الانسحاب أيضا انسحابا من جميع الوثائق السابقة ولا ينتج أثره إلا بالنسبة للدولة التي قامت به، وتظل الاتفاقية سارية وواجبة النفاذ بالنسبة لدول الاتحاد الأخرى.

(٣) يكون الانسحاب نافذا بعد سنة من تاريخ تسلم المدير العام للإخطار.

(٤) لا يجوز لأية دولة أن تمارس حق الانسحاب المنصوص عليه في هذه المادة قبل انقضاء خمس سنوات من التاريخ الذي أصبحت فيه عضوا في الاتحاد.

#### مادة ٣٦

تطبيق الاتفاقية: (١) التزام اعتماد الإجراءات اللازمة (٢) تاريخ قيام هذا الالتزام.

(١) تتعهد كل دولة طرف في هذه الاتفاقية بأن تتخذ، وفقا لدستورها، الإجراءات اللازمة لضمان تنفيذ هذه الاتفاقية.

(٢) من المتفق عليه أنه يجب، عندما تصبح دولة ملتزمة بهذه الاتفاقية، أن تكون في وضع يسمح لها، وفقا لتشريعها الداخلي، بأن تضع أحكام هذه الاتفاقية موضع التنفيذ.

#### مادة ٣٧

الأحكام الختامية: (١) لغات الوثيقة (٢) التوقيع (٣) صورة رسمية مطابقة للأصل (٤) التسجيل (٥) الاخطارات.

(١) (أ) توقع هذه الوثيقة من نسخة وحيدة باللغتين الإنجليزية والفرنسية، وتودع لدى المدير العام مع مراعاة الفقرة (٢).

(ب) يضع المدير العام نصوصاً رسمية باللغات العربية والألمانية والإيطالية والبرتغالية والإسبانية وبأية لغات أخرى تحددها الجمعية، وذلك بعد التشاور مع الحكومات المعنية.

(ج) في حالة الخلاف على تفسير النصوص المختلفة تكون الحجية للنص الفرنسي.

(د) تظل هذه الوثيقة مفتوحة للتوقيع حتى ٣١ يناير ١٩٧٢. وحتى هذا التاريخ، تكون النسخة المشار إليها في الفقرة ١ (أ) مودعة لدى حكومة الجمهورية الفرنسية.

(٣) يرسل المدير العام نسختين معتمدين من النص الموقع لهذه الوثيقة إلى حكومات جميع دول الاتحاد وإلى حكومة أية دولة أخرى بناء على طلبها.

(٤) يتولى المدير العام تسجيل هذه الوثيقة لدى سكرتارية الأمم المتحدة.

(٥) يتولى المدير العام إخطار حكومات جميع دول الاتحاد بالتوقيعات وإيداعات وثائق التصديق أو الانضمام وأية إعلانات وإرادة في هذه الوثائق أو صادرة طبقاً للمواد ٢٨(١)(ج)، ٣٠(٢)(أ) و(ب)، ٢٣(٢)، وببديء نفاذ أية أحكام لهذه الوثيقة، وبإخطارات الانسحاب والإخطارات التي تتم وفقاً للمواد ٣٠(٢)(ج)، ٣١(١)، و(٢)، ٣٣(٣)، ٣٨(١)، وكذلك الإخطارات المشار إليها في الملحق.

#### مادة ٣٨

أحكام انتقالية: (١) ممارسة " امتياز الخمس سنوات " (٢) مكتب الاتحاد، مدير المكتب (٣) مآل مكتب الاتحاد.

(١) لدول الاتحاد التي لم تصدق على هذه الوثيقة أو لم تنضم إليها وغير الملزمة بالمواد من ٢٢ إلى ٢٦ من وثيقة استكهولم أن تمارس، حتى ٢٦ أبريل ١٩٧٥، إذا رغبت في ذلك، الحقوق المنصوص عليها في هذه المواد كما لو كانت ملتزمة بها. وتقوم أية دولة ترغب في ممارسة تلك

الحقوق بإيداع إخطار كتابي بذلك لدى المدير العام، ويكون هذا الإخطار ساريا من تاريخ تسلمه، وتعتبر تلك الدول أعضاء في الجمعية حتى انقضاء المدة المذكورة.

(٢) ويمارس أيضا المكتب الدولي للمنظمة وظيفة مكتب الاتحاد والمدير العام وظيفة مدير المكتب المذكور ما دامت جميع دول الاتحاد لم تصبح أعضاء في المنظمة.

(٣) تؤول حقوق والتزامات وأموال مكتب الاتحاد إلى المكتب الدولي للمنظمة بمجرد أن تصبح جميع دول الاتحاد أعضاء في المنظمة.

## ملحق

### أحكام خاصة بشأن البلدان النامية

#### المادة الأولى

الإمكانيات الممنوحة للبلدان النامية: (١) إمكانية المطالبة بالإفادة من بعض الحقوق، الإعلان (٢) مدة صلاحية الإعلان (٣) البلدان التي لم تعد تعتبر من البلدان النامية (٤) مخزون النسخ المتوفرة (٥) الإعلانات المتعلقة ببعض الأقاليم (٦) حدود المعاملة بالمثل.

(١) لكل دولة، تعتبر دولة نامية وفقا لما يجرى به العمل في الجمعية العامة للأمم المتحدة، تصدق على هذه الوثيقة، التي يشكل هذا الملحق جزءا لا يتجزأ منها، أو تنضم إليها، والتي نظرا لوضعها الاقتصادي واحتياجاتها الاجتماعية أو الثقافية لا تعتبر نفسها في الوقت الحاضر في مركز يمكنها من اتخاذ الإجراءات المناسبة لضمان حماية كل الحقوق بالوضع الوارد في هذه الوثيقة، أن تعلن بأنها ستستعمل الحق المنصوص عليه في المادة الثانية أو ذلك المنصوص عليه في المادة الثالثة أو كليهما معا، وذلك بموجب إخطار نودعه لدى المدير العام عند إيداع وثيقة تصديقها أو انضمامها، أو مع مراعاة المادة الخامسة (١) (ج) في أى وقت لاحق. كما يمكنها بدلا من استعمال الحق المنصوص عليه في المادة الثانية الإدلاء بإعلان طبقا للمادة الخامسة (١) (أ).

(٢) (أ) كل إعلان وفقا للفقرة (١) يتم إخطاره قبل انقضاء فترة عشر سنوات اعتبارا من تاريخ العمل بالمواد من ١ إلى ٢١ وبهذا الملحق طبقا للمادة ٢٨ (٢)، يظل نافذا حتى نهاية المدة المذكورة. ويمكن أن يتجدد كليا أو جزئيا لمدد أخرى متتالية طول كل منها عشر سنوات وذلك بإخطار

يودع لدى المدير العام خلال مهلة لا تزيد عن خمسة عشر شهرا ولا تقل عن ثلاثة أشهر قبل انقضاء فترة العشر سنوات الجارية.

(ب) كل إعلان وفقا للفقرة (١) يتم إخطاره بعد انتهاء فترة عشرة سنوات من العمل بالمواد من ١ إلى ٢١ وبهذا الملحق طبقا للمادة ٢٨(٢)، يظل نافذا حتى نهاية فترة العشر سنوات الجارية، ويمكن تجديده على النحو الوارد في الجملة الثانية من الفقرة الفرعية (أ).

(٣) لا يحق لأية دولة الاتحاد لم تعد تعتبر دولة نامية على النحو الموضح بالفقرة (١) أن تجدد إعلانها طبقا لما تقتضي به الفقرة (٢). وسواء سحبت هذه الدولة إعلانها رسميا أو لم تسحبه، فإنه لا يحق لها الاستفادة من الحقوق المنصوص عليها في الفقرة (١) إما في نهاية فترة السنوات العشر الجارية وإما بعد الكف عن اعتبارها بلدا ناميا بثلاث سنوات، أي الأجلين أطول.

(٤) إذا ما وحد مخزون من نسخ تم إنتاجها بمقتضى ترخيص ممنوح طبقا لأحكام هذا الملحق، وذلك عندما يكف الإعلان الصادر طبقا للفقرة (١) أو الفقرة (٢) عن النفاذ، فإنه يجوز الاستمرار في توزيع مثل هذه النسخ حتى نفاذها.

(٥) يجوز لكل دولة تلتزم بأحكام هذه الوثيقة وتكون قد أودعت إعلانا أو إخطارا طبقا للمادة ٣١(١) بخصوص تطبيق هذه الوثيقة على إقليم معين يمكن أن تعتبر حالته مماثلة لحالة الدول المنصوص عليها بالفقرة (١)، أن تصدر الإعلان المشار إليه في الفقرة (١) والإخطار بالتجديد المشار إليه في الفقرة (٢) بالنسبة لهذا الإقليم. وطالما ظل مثل هذا الإعلان أو الإخطار نافذا، فإن أحكام هذا الملحق تنطبق على الإقليم الذي صدر بصنده.

(٦) (أ) إن واقعة استعمال إحدى الدول لأحد الحقوق المشار إليها في الفقرة (١) لا تجيز لدولة أخرى أن تمنح للمصنعات التي تكون دولة منشئها هي



الدولة الأولى حماية أقل مما هو مفروض عليها منحه طبقا للمواد من ١ إلى ٢٠.

(ب) لا يمكن ممارسة حق المعاملة بالممثل المنصوص عليه في الجملة الثانية من المادة ٣٠(٢) (ب) حتى تاريخ إنقضاء الفترة الجارية وفقا للمادة الأولى (٣)، وذلك بالنسبة للمصنفات التي تكون دولة منشئها هي إحدى الدول التي أصدرت إعلانا وفقا للمادة الخامسة (١)(أ).

### المادة الثانية

تقييد حق الترجمة: (١) إمكانية منح تراخيص من قبل السلطة المختصة إلى (٤) شروط منح التراخيص (٥) الأغراض التي تمنح من أجلها التراخيص (٦) انتهاء صلاحية التراخيص (٧) المصنفات التي تتألف أساسا من صور توضيحية (٨) المصنفات التي تسحب من التداول (٩) منح تراخيص لهيئات الإذاعة.

(١) فيما يتعلق بالمصنفات المنشورة في شكل مطبوع أو في أي شكل مماثل آخر من أشكال الاستساخ، يحق لكل دولة تكون قد أعلنت بأنها ستستعمل الحق المنصوص عليه في هذه المادة أن تستبدل بالحق الاستثنائي للترجمة المنصوص عليه في المادة ٨، نظاما للتراخيص غير الاستثنائي والغير قابلة للتحويل، تمنحها السلطة المختصة وفقا للشروط التالية وطبقا للمادة الرابعة.

(٢) (أ) مع مراعاة الفقرة (٣)، إذا ما انقضت فترة ثلاثة سنوات أو أية فترة أطول يحددها التشريع الوطني للدولة المذكورة، اعتبارا من تاريخ أول نشر لمصنف، دون أن تنشر ترجمة لهذا المصنف بلغة عامة التداول في هذه الدولة بواسطة صاحب حق الترجمة أو بتصريح منه، فإن أيا من مواطني هذه الدولة يمكنه الحصول على ترخيص بترجمة المصنف إلى

اللغة المذكورة ونشر هذه الترجمة في شكل مطبوع أو في أي شكل مماثل آخر من أشكال النقل.

(ب) يمكن أيضا منح ترخيص وفقا لهذه المادة إذا ما نفذت جميع الطبعات للترجمة المنشورة باللغة المذكورة.

(٣) (أ) في حالة الترجمة إلى لغة ليست عامة التداول في دولة أو أكثر من الدول المتقدمة الأعضاء في الاتحاد تستبدل فترة الثلاث سنوات المنصوص عليها في الفقرة (٣)(أ) بفترة سنة.

(ب) لكل دولة مشار إليها في الفقرة (١)، باتفاق إجماعي من جانب الدول المتقدمة الأعضاء في الاتحاد والتي لها نفس اللغة المتداولة، أن تستبدل، في حالة الترجمات إلى تلك اللغة، بفترة الثلاث سنوات المشار إليها في الفقرة (٢)(أ) فترة أقصر تحدد طبقا للاتفاق المذكور على ألا تقل هذه الفترة عن سنة واحدة. ومع ذلك، لا تنطبق أحكام الجملة السابقة إذا كانت اللغة المعنية هي الإنجليزية أو الفرنسية أو الإسبانية. هذا وأي اتفاق من هذا القبيل يخطر به المدير العام من جانب الحكومات التي عقده.

(٤) (أ) لا يمنح أي ترخيص بمقتضى هذه المادة إلا بعد انقضاء مهلة إضافية قدرها سنة أشهر في حالة التراخيص التي يمكن الحصول عليها بعد انقضاء فترة ثلاثة سنوات، وتسعة أشهر في حالة التراخيص التي يمكن الحصول عليها بعد انقضاء عام واحد وذلك:

(١) اعتبارا من التاريخ الذي يستوفى فيه الطالب الإجراءات المنصوص عليها في المادة الرابعة (١).

(٢) أو في حالة عدم الاستدلال على شخصية صاحب حق الترجمة أو عنوانه، من التاريخ الذي يرسل فيه الطالب، طبقا لما تقتضي به المادة الرابعة (٢)، نسخا من طلبه المقدم للسلطة المختصة بمنح الترخيص.

(ب) لا يمنح ترخيص بمقتضى هذه المادة إذا نشرت ترجمة إلى اللغة التي قدم الطلب من أجلها من جانب صاحب حق الترجمة أو بتصريح منه خلال مهلة الستة أو التسعة أشهر.

(٥) لا يمنح ترخيص بمقتضى هذه المادة إلا لأغراض التعليم المدرسي أو الجامعي أو لأغراض البحوث.

(٦) تنتهي صلاحية كل ترخيص يكون قد منح وفقا لهذه المادة إذا نشرت ترجمة للمصنف من جانب صاحب حق الترجمة أو بتصريح منه بثمن مقارب للثمن المعتاد في الدولة المعنية بالنسبة للمصنفات المماثلة، وذلك إذا ما كانت هذه الترجمة باللغة نفسها ولها في الجوهر ذات مضمون الترجمة المنشورة بمقتضى الترخيص. أما النسخ التي يتم إنتاجها قبل انتهاء أجل الترخيص فيجوز استمرار تداولها حتى نفاذها.

(٧) بالنسبة للمصنفات التي تتألف أساسا من صور توضيحية، لا يمنح ترخيص لعمل ونشر ترجمة للنص ولا لنقل ونشر الصور التوضيحية إلا إذا استوفيت أيضا الشروط المنصوص عليها في المادة الثالثة.

(٨) لا يمنح أي ترخيص وفقا لهذه المادة عندما يسحب المؤلف من التداول جميع نسخ مصنفه.

(٩) (أ) يجوز أيضا منح ترخيص بترجمة مصنف يكون قد نشر في شكل مطبوع أو في أي شكل آخر مماثل من أشكال النقل، لأي هيئة إذاعية يقع مقرها الرئيسي في إحدى الدول المشار إليها في الفقرة (١)، وذلك بناء على طلب تقدمه تلك الهيئة إلى السلطة المختصة في الدولة المذكورة بشرط مراعاة جميع الشروط التالية:

(١) أن تتم الترجمة من نسخة منتجة ومقتناة وفقا لقوانين الدولة المذكورة.

(٢) ألا تستخدم الترجمة إلا في إذاعات يقتصر هدفها على خدمة أغراض التعليم وإذاعة معلومات ذات طابع علمي موجهة إلى الخبراء في مهنة معينة.

(٣) ألا تستخدم الترجمة إلا للأغراض المشار إليها في الشرط الوارد بالبند (٢) عاليه، ومن خلال إذاعات مشروعة موجهة لمستمعين في إقليم الدولة المذكورة، بما في ذلك الإذاعات التي تتم عن طريق تسجيلات صوتية أو بصرية أعدت بطرق مشروعة من أجل هذه الإذاعات دون سواها.

(٤) أن تتجرد جميع أوجه استخدام الترجمة من قصد الربح.

(ب) يجوز كذلك استعمال التسجيلات الصوتية أو البصرية لترجمة أعدتها هيئة إذاعية بمقتضى ترخيص منح وفقاً لهذه الفقرة، وبناء على موافقة هذه الهيئة، بواسطة أية هيئة إذاعية أخرى يكون مقرها الرئيسي في الدولة التي منحت سلطتها المختصة الترخيص المذكور، وذلك للأغراض وطبقاً للشروط المشار إليها في الفقرة الفرعية (أ).

(ج) مع مراعاة الوفاء بكل المعايير والشروط المذكورة بالفقرة الفرعية (أ)، يجوز أيضاً الترخيص لهيئة إذاعية بترجمة أى نص مضمن في تثبيت سمعي بصرى أعد ونشر ليستخدم في أغراض التعليم المدرسي أو الجامعي وحدها.

(د) مع مراعاة الفقرات الفرعية من (أ) إلى (ج)، تنطبق أحكام الفقرات السابقة على منح واستعمال أى ترخيص يكون قد منح طبقاً لهذه الفقرة.

### المادة الثالثة

تفويض حق الاستئساخ: (١) إمكانية منح التراخيص من قبل السلطة المختصة (٢) إلى (٥) شروط منح هذه التراخيص (٦) إنتهاء صلاحية التراخيص (٧) المصنفات التي تنطبق عليها هذه المادة.

(١) لكل دولة تعلن بأنها ستستعمل الحقوق المنصوص عليها في هذه المادة أن تستبدل بالحق الاستثنائي للاستساخ المنصوص عليه في المادة ٩ نظام للتأخييص غير الاستثنائية وغير القابلة للتحويل تقوم بمنحها السلطة المختصة بالشروط التالية ووفقا للمادة الرابعة.

(٢) (أ) فيما يتعلق بالمصنف الذي تطبق عليه هذه المادة بموجب الفقرة (٧) وعند انقضاء:

(١) الفترة المجددة في الفقرة (٣) محسوبة ابتداء من تاريخ أول نشر لطبعة معينة من هذا المصنف: أو

(٢) أية فترة أطول يحددها التشريع الوطني للدولة المشار إليها في الفقرة (١) ومحسوبة اعتبارا من نفس التاريخ.

إذا لم تكن نسخ من تلك الطبعة قد طرحت للتداول في هذه الدولة من جانب صاحب حق النقل أو بتصريح منه تلبية لاحتياجات عامة الجمهور أو التعليم المدرسي والجامعي بثمن مقارب للثمن المعتاد في الدولة المذكورة بالنسبة لمصنفات مماثلة، فلائى من رعايا هذه الدولة أن يحصل على ترخيص لاستساخ ونشر هذه الطبعة بالسعر المذكور أو بسعر يقل عنه تلبية لاحتياجات التعليم المدرسي والجامعي.

(ب) يجوز أيضا منح ترخيص لنقل ونشر طبعة طرحت للتداول على النحو الوارد في الفقرة الفرعية (أ) طبقا للشروط الواردة في هذه المادة وذلك إذا توقف لمدة ستة أشهر، بعد انتهاء المدة السارية، عرض نسخ مرخصة من هذه الطبعة للبيع في الدولة المعنية تلبية لاحتياجات الجمهور أو للتعليم المدرسي والجامعي بسعر مقارب للسعر المعتاد في تلك الدولة لمصنفات مماثلة.

(٣) مدة الفترة المشار إليها بالفقرة (٣)(أ) خمس سنوات، على أن يستثنى من ذلك:

(أ) المصنفات فى العلوم الرياضية والطبيعية والتكنولوجية، فتكون الفترة بالنسبة لها ثلاث سنوات.

(ب) المصنفات التى تنتمى إلى عالم الخيال، كالروايات والمؤلفات الشعرية والمسرحية والموسيقية، وكتب الفن، فتكون الفترة بالنسبة لها سبع سنوات.

(٤) (أ) فى حالة الترخيص الذى يمكن الحصول عليه بعد انقضاء ثلاث سنوات، لا يمنح الترخيص إلا بعد انقضاء فترة ستة أشهر:

(١) من تاريخ استيفاء الطالب للإجراءات المنصوص عليها فى المادة الرابعة (١)، أو

(٢) فى حالة عدم الاستدلال على شخصية صاحب حق النقل أو عنوانه، من التاريخ الذى يرسل فيه الطالب، كما تقضى بذلك المادة الرابعة (٢)، نسخاً من طلبه إلى السلطة المختصة بمنح الترخيص.

(ب) لا يجوز منح ترخيص فى الحالات الأخرى، وبشرط انطباق المادة الرابعة (٢)، قبل انقضاء فترة ثلاثة أشهر تحتسب من تاريخ إرسال نسخ الطلب.

(ج) لا يجوز منح أى ترخيص وفقاً لهذه المادة إذا حصل عرض للبيع على النحو الوارد فى الفقرة (٢) (أ) خلال مدتي الستة أو الثلاثة أشهر المشار إليهما فى الفقرتين الفرعيتين (أ) و(ب).

(د) لا يجوز منح أى ترخيص إذا سحب المؤلف من التداول كل نسخ الطبعة التى طلب الترخيص من أجل نقلها أو نشرها.

(٥) لا يمنح بمقتضى هذه المادة ترخيص بنقل ونشر ترجمة لمصنف ما فى الحالتين التاليتين:

(١) إذا لم تكن الترجمة المشار إليها قد نشرت من جانب صاحب حق الترجمة أو بتصريح منه.

(٢) إذا لم تكن الترجمة بلغة عامة التداول فى الدولة التى طلب فيها الترخيص.

(٦) إذا طرحت للتداول فى الدولة المشار إليها فى الفقرة (١) من جانب صاحب حق النقل أو بتصريح منه نسخ من طبعة لمصنف ما تلبية لاحتياجات عامة الجمهور أو التعليم المدرسي والجامعي، بثمن مقارب للثمن المعتاد فى تلك الدولة بالنسبة لمصنفات مماثلة، فإن كل ترخيص منح بمقتضى هذه المادة تنتهي صلاحيته إذا كانت هذه الطبعة باللغة نفسها ولها فى الجوهر ذات مضمون الطبعة المنشورة بمقتضى الترخيص، أما النسخ التى يكون قد تم إنتاجها قبل انتهاء صلاحية الترخيص فيجوز استمرار تداولها حتى نفاذها.

(٧) (أ) مع مراعاة الفقرة الفرعية (ب) تقتصر المصنفات التى تنطبق عليها هذه المادة على المصنفات المنشورة فى شكل مطبوع أو فى أى شكل مماثل آخر من أشكال النقل.

(ب) تنطبق هذه المادة أيضا على النقل السمعي البصري لتسجيلات سمعية بصرية مشروعة باعتبارها تشكّل أو تحتوى على أعمال محمية، كما تنطبق على ترجمة النص المصاحب لها إلى لغة عامة التداول بالدولة التى يطلب فيها الترخيص، وذلك بشرط أن تكون التسجيلات السمعية البصرية المعنية قد أعدت ونشرت لأغراض التعليم المدرسي والجامعي دون سواها.

#### المادة الرابعة

أحكام مشتركة بشأن التراخيص المنصوص عليها فى المادتين الثانية والثالثة: (١) و(٢) الإجراءات (٣) بيان اسم المؤلف وعنوان المصنف (٤) تصدير النسخ (٥) إشارة (٦) المكافأة.

(١) لا يمنح الترخيص طبقا للمادة الثانية أو للمادة الثالثة إلا إذا أثبت الطالب وفقا للإجراءات المعمول بها في الدول المعنية أنه طلب من صاحب الحق التصريح بعمل ونشر الترجمة أو بنقل ونشر الطبعة حسبما كانت الحالة فرفض طلبه، أو أنه لم يتمكن من العثور على صاحب الحق بعد بذل الجهود اللازمة. وعلى الطالب في نفس الوقت الذي يقدم فيه الطلب أن يخطر به أى مركز إعلامي وطني أو دولي مشار إليه في الفقرة (٢).

(٢) إذا لم يتسن لطالب الترخيص العثور على صاحب الحق فعليه أن يرسل بالبريد الجوى الموصى عليه صورا من طلبه الذى تقدم به إلى السلطة المختصة بمنح الترخيص إلى الناشر الذى يظهر اسمه على المصنف وإلى أى مركز إعلام وطني أو دولي يكون قد تعين فى إخطار يودع لهذا الغرض لدى المدير العام بمعرفة حكومة الدولة التى يعتقد أن الناشر يمارس فيها الجانب الأكبر من نشاطه.

(٣) يجب أن يذكر اسم المؤلف على جميع نسخ الترجمة أو ما ينقل وينشر من المصنف فى ظل ترخيص ممنوح طبقا لأحكام المادة الثانية أو المادة الثالثة. ويجب أن يظهر عنوان المصنف على جميع مثل هذه النسخ، وبالنسبة للترجمة يجب أن يظهر العنوان الأصلي للمصنف فى كل الحالات على جميع النسخ المذكورة.

(٤) (أ) لا يمتد الترخيص الممنوح وفقا للمادة الثانية أو للمادة الثالثة إلى تصدير النسخ، ولا يسرى مثل هذا الترخيص إلا على نشر الترجمة أو ما ينقل من المصنف حسب الأحوال داخل إقليم الدولة التى طلب فيها الترخيص.

(ب) فى تطبيق أحكام الفقرة الفرعية (أ)، يجب أن يعتبر تصديرا إرسال نسخ من أى إقليم إلى الدولة التى أصدرت طبقا للمادة الأولى (٥) تصريحاً بشأن ذلك الإقليم.



(ج) إذا أرسلت هيئة حكومية أو أية هيئة عامة أخرى فى دولة منحت بمقتضى المادة الثانية ترخيصا بترجمة مصنف إلى لغة غير الإنجليزية أو الفرنسية أو الإسبانية، نسخا إلى بلد آخر من ترجمة نشرت بناء على هذا الترخيص، فإن هذا الإرسال لا يعد فى تطبيق الفقرة الفرعية (أ) تصديرا إذا روعيت كل الشروط الآتية:

(١) أن يكون المرسل إليهم أفرادا من رعايا الدولة التى منحت سلطتها المختصة بالترخيص، أو منظمات أعضاؤها من هؤلاء الرعايا.

(٢) ألا تستخدم النسخ إلا فى أغراض التعليم المدرسي أو الجامعي أو لأغراض البحوث.

(٣) ألا يكون الغرض من إرسال النسخ وتوزيعها بعد ذلك على المرسل إليهم تحقيق أى ربح.

(٤) أن يعقد بين البلد الذى ترسل إليه النسخ والدولة التى منحت سلطتها المختصة بالترخيص اتفاقا يسمح بالاستلام أو التوزيع أو بهما معا، وأن تكون حكومة هذه الدولة التى منحت الترخيص قد أخطرت المدير العام بهذا الاتفاق.

(٥) كل نسخة تنشر وفقا لترخيص ممنوح بمقتضى المادة الثانية أو المادة الثالثة يجب أن تحمل باللغة المناسبة نصا يفيد أن النسخة ليست مطروحة للتداول إلا فى الدولة أو الإقليم الذى ينطبق عليه الترخيص.

(٦) (أ) تتخذ على المستوى الوطني التدابير الكفيلة بضمان ما يلي:

(١) إن ينص الترخيص، لمصلحة صاحب حق الترجمة أو النقل حسبما كان الحال، على مكافأة عادلة تتفق وما يستحق عادة فى حالة

التراخيص التى تسفر عنها مفاوضات حرة بين ذوى الشأن فى  
البلدين المعنيين.

(٢) أن تدفع المكافأة وترسل. وإذا اعترضت ذلك لوائح وطنية لتنظيم  
النقد، فعلى الجهة المختصة ألا تدخر وسعا فى اللجوء إلى الأجهزة  
الدولية لتأمين إرسال قيمة المكافأة بعملة دولية قابلة للتحويل أو ما  
يعادلها.

(ب) يتخذ التشريع الوطني التدابير الكفيلة بضمان ترجمة صحيحة للمصنف  
ونقل دقيق للطبعة المعنية وذلك حسبما كان الحال.

#### المادة الخامسة

إمكانية أخرى لتقييد حق الترجمة: (١) النظام المنصوص عليه فى وثيقتي  
عام ١٨٨٦ و ١٨٩٦ (٢) عدم جواز تغيير النظام بعد اختيار النظام  
المنصوص عليه فى المادة الثانية (٣) مهلة اختيار النظام الآخر.

(١) (أ) عند التصديق على هذه الوثيقة أو الانضمام إليها، يمكن لكل دولة  
يكون من حقها الإعلان بأنه ستستعمل الحق المنصوص عليه فى المادة  
الثانية أن تبدى بدلا من ذلك:

(١) إذا كانت دولة تنطبق عليها المادة ٣٠(٢)(أ)، إعلانا وفقا لهذا النص  
فيما يتعلق بحق الترجمة.

(٢) إذا كانت دولة لا تنطبق عليها المادة ٣٠(٢)(أ)، وحتى إذا لم تكن  
دولة خارج الاتحاد، إعلانا على النحو الوارد فى الجملة الأولى من  
المادة ٣٠(٢)(ب).

(ب) فى حالة الدولة التى لم تعد تعتبر دولة نامية على النحو المشار إليه  
فى المادة الأولى (١) يظل الإعلان الصادر وفقاً لهذه الفقرة صالحا حتى  
تاريخ انتهاء المدة السارية طبقاً للمادة الأولى (٣).

(ج) لا يجوز لأية دولة تكون قد أصدرت إعلانا طبقا لهذه الفقرة أن تستعمل فيما بعد الحق المنصوص عليه في المادة الثانية حتى ولو سحبت الإعلان المذكور.

(٢) مع مراعاة أحكام الفقرة (٣)، لا يجوز لأية دولة تكون قد استعملت الحق المنصوص عليه في المادة الثانية، أن تصدر بعد ذلك إعلانا طبقا للفقرة (١).

(٣) يمكن لأية دولة لم تعد تعتبر دولة نامية على النحو المشار إليه في المادة الأولى (١). أن تصدر في فترة أقصاها سنتان قبل انقضاء المدة السارية وفقا للمادة الأولى (٣)، إعلانا وفقا لمفهوم الجملة الأولى من المادة ٣٠ (٢) (ب) وذلك بالرغم من واقعة كونها دولة ليست خارج الاتحاد. ويصبح مثل هذا الإعلان نافذا في التاريخ الذي تنتهي فيه الفترة السارية وفقا للمادة الأولى (٣).

#### المادة السادسة

إمكانية تطبيق أو قبول تطبيق بعض أحكام الملحق قبل الالتزام به: (١) الإعلان (٢) أمين الإيداع وتاريخ بدء أثر الإعلان).

(١) تستطيع كل دولة من دول الاتحاد أن تعلن، اعتبارا من تاريخ هذه الوثيقة وفي أي وقت قبل أن تصبح ملتزمة بأحكام المواد من ١ إلى ٢١ وبهذا الملحق، الآتي:

(١) إذا كانت من الدول التي لو كانت ملتزمة بالمواد من ١ إلى ٢١ وبهذا الملحق لكان لها أن تستعمل الحقوق المنصوص عليها في المادة الأولى (١)، بأنها ستطبق أحكام المادة الثانية أو أحكام المادة الثالثة أو كليهما معا على المصنفات التي تكون دولة منشئها دولة قد قبلت، طبقا لأحكام البند (٢) المذكور فيما بعد، تطبيق هاتين المادتين على مثل هذه

المصنفات أو التي تكون مرتبطة بالمواد من ١ إلى ٢١ وبهذا الملحق.  
ويمكن إسناد مثل هذا الإعلان إلى المادة الخامسة بدلا من المادة الثانية.  
(٢) بأنها تقبل تطبيق هذا الملحق على المصنفات التي تكون هي دولة منشئها  
وذلك من جانب الدول التي أصدرت إعلانا طبقا للبند (١) عاليه أو  
أودعت إخطارا طبقا للمادة الأولى.  
(٣) كل إعلان يصدر وفقا للفقرة (١) يجب أن يكون كتابة كما يجب أن  
يودع لدى المدير العام. وينتج الإعلان أثره من تاريخ إيداعه.

**ثانيا**

**مبادئ توجيهية لتنظيم  
ملفات البيانات الشخصية  
المعدة بالحاسبات الإلكترونية**



**مبادئ توجيهية لتنظيم ملفات**  
**البيانات الشخصية المعدة بالحاسبات الإلكترونية**  
**ألف: المبادئ التي تنص علي ضمانات دنيا**  
**يجب إدخالها في التشريعات الوطنية**

**١- مبدأ المشروعية والنزاهة:**

ينبغي عدم جمع المعلومات المتعلقة بالأشخاص أو تجهيزها بأساليب غير  
نزيفة أو غير مشروعة أو استخدامها لأغراض مخالفة لمقاصد ميثاق الأمم  
المتحدة ومبادئه.

**٢- مبدأ الصحة:**

يلتزم المسؤولون عن إعداد ملفات البيانات أو المسؤولون عن حفظها  
بالتحقق من دقة البيانات المسجلة وملاءمتها والعمل علي استكمالها بانتظام أو  
لدى استخدام المعلومات التي تحتويها الملفات.

**٢- مبدأ تحديد الغاية:**

ينبغي أن تكون الغاية التي أنشئ الملف من أجلها محددة ومشروعة  
ومعلنة قبل إنشائه حتى يتسني فيها بعد التحقق من:

أ- أن جميع البيانات الشخصية التي جمعت وسجلت لا تزال صلة بالغاية  
المستهدفة.

ب- أن أيا من البيانات الشخصية المذكورة لا يستخدم أو يفشي، لغايات  
لا تتفق مع الغايات المحددة، إلا بموافقة الشخص المعني.

ج- أن مدة حفظ البيانات لشخصية لا تتجاوز لمدة التي تتيح بلوغ الغاية المحددة.

#### ٤- مبدأ وصول الأشخاص المعنيين إلى الملفات:

من حق أي شخص يثبت شخصيته، أيا كانت جنسيته أو محل إقامته، أن يعرف ما إذا كانت تجري معالجة آلية لبيانات تتعلق به، وأن يخطر بذكر بشكل مفهوم، دون تأخير أو رسوم لا داعي لهما، وأن يلبي طلبه بإجراء عمليات التصويب أو المحو الملائمة في حالة البيانات التي تقتدر إلى المشروعية أو اللزوم أو الدقة، وينبغي توخي سبيل للانتصاف. وفي حالة التصويب تكون التكاليف على نفقة المسؤول عن الملف.

#### ٥- مبدأ عدم التمييز:

فيما عدا حالات الاستثناء المنصوص عليها على سبيل الحصر تحت المبدأ (٦) لا يجوز تسجيل البيانات التي من شأنها أن تؤدي إلى تمييز غير مشروع أو تعسفي، وعلى وجه خاص المعلومات المتعلقة بالأصل العرقي أو الإثني أو اللون أو الحياة الجنسية أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو غيرها وكذلك الانتماء إلى الجمعيات أو النقابات.

#### ٦- سلطة الاستثناء:

لا يجوز السماح باستثناءات للمبادئ من (١) إلى (٤) إلا إذا كانت ضرورية لحماية الأمن الوطني أو النظام العام أو الصحة أو الأخلاق العامة أو حقوق وحريات الآخرين، وعلى وجه خاص الأشخاص المضطهدين، وكان منصوصا عليها صراحة في قانون أو في قواعد مماثلة موضوعية وفقا للنظام القانوني الداخلي الذي يحدد صراحة حدودها وينص على الضمانات المناسبة.

وفيما يتعلق بالاستثناءات للمبدأ (٥) المتعلق بحظر التمييز، فبالإضافة إلى ضرورة إخضاعها لنفس الضمانات المنصوص عليها فيما يتعلق بالاستثناءات للمبادئ من (١) إلى (٤)، لا يجوز السماح بها إلا في نطاق



الحدود المنصوص عليها في الشريعة الدولية لحقوق الإنسان وغيرها من الصكوك ذات الصلة في ميدان حماية حقوق الإنسان ومنع التمييز.

#### ٧- مبدأ الأمن:

ينبغي اتخاذ التدابير الملائمة لحماية الملفات سواء ضد المخاطر الطبيعية، مثل فقدانها عرضيا أو تلفها، أو المخاطر البشرية مثل الاطلاع عليها بغير إذن أو استخدام البيانات بشكل غير أمين.

#### ٨- الرقابة والعقوبات:

ينبغي أن يحدد قانون كل بلد السلطة المكلفة بمراقبة مراعاة المبادئ السالف الذكر، وفقا للنظام القانوني الداخلي. وينبغي أن توفر هذه السلطة ضمانات الحياد والكفاءة التقنية. وفي حالة انتهاك أحكام القانون الداخلي المنفذة للمبادئ المذكورة، ينبغي توخي عقوبات جنائية وكذلك سبل الانتصاف الملائمة.

#### ٩- تدفق البيانات عبر الحدود:

عندما توفر التشريعات في بلدين أو عدة بلدان معنية بتدفق البيانات عبر الحدود ضمانات متساوية، نوعا ما، فيما يتعلق بحماية الحياة الخاصة، ينبغي أن يكون بالإمكان أن تنتقل المعلومات بنفس الحرية التي تنتقل بها داخل كل من هذه الأقاليم المعنية، وفي حالة عدم وجود ضمانات متبادلة، لا يجوز أن يقبل علي غير وجه حق وضع حدود لهذا الانتقال، ولا يقبل ذلك إلا بقدر ما تقتضيه حماية الحياة الخاصة.

#### ١٠- نطاق التطبيق:

ينبغي أن تطبق هذه المبادئ في المقام الأول علي جميع الملفات العامة والخاصة المعالجة آليا، بما في ذلك، شريطة إجراء التكييف الملائم، الملفات التي تعالج يدويا، وينبغي أيضا وضع أحكام خاصة، اختياريًا، لتوسيع نطاق

تطبيق جميع هذه المبادئ أو جزء منها، ليشمل ملفات الأشخاص المعنويين طالما احتوت في جزء منها علي معلومات تتعلق بأشخاص طبيعيين.

### **باء: تطبيق المبادئ التوجيهية علي الملفات التي**

#### **تحتوي علي بيانات ذات طابع شخصي،**

#### **والتي تحتفظ بها المنظمات الحكومية الدولية**

ينبغي أن تكون المبادئ التوجيهية قابلة للتطبيق علي الملفات التي تحتوي علي بيانات ذات طابع شخصي والتي تحتفظ بها المنظمات الحكومية الدولية بشرط القيام بالتكيف اللازم لكي توضع في الاعتبار الاختلافات التي يمكن أن تكون قائمة بين الملفات الداخلية، المتعلقة بالمعاملين ومن في حكمهم، والملفات الخارجية المتعلقة بأطراف ثالثة علي علاقة بالمنظمة.

ويجوز النص، بالتحديد، علي استثناء لهذه المبادئ (حكم إنساني) إذا كانت الغاية من الملف هي حماية حقوق الإنسان والحريات الأساسية للشخص المعني أو المساعدة الإنسانية. وينبغي لكل منظمة أن تعين السلطة المختصة قانونا لمراقبة مراعاة هذه المبادئ التوجيهية.

وينبغي أن تنص القوانين التشريعية الوطنية علي حكم من نفس النوع بالنسبة للمنظمات الدولية غير الحكومية التي ينطبق عليها هذا القانون، وكذلك بالنسبة للمنظمات الحكومية الدولية التي لم يستبعد الاتفاق الخاص بمقرها تطبيق القوانين التشريعية الوطنية المذكورة.

### **ثالثاً**

**مقررات وتوصيات المؤتمر الخامس عشر  
للجمعية الدولية لقانون العقوبات بشأن  
جرائم الكمبيوتر**



## مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية

### لقانون العقوبات بشأن جرائم الكمبيوتر

#### أولاً: في الشق الموضوعي - الجرائم

لقد أوصى المؤتمر بأن تتضمن قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر ما يلي:

١- الاحتيال أو الغش المرتبط بالكمبيوتر: ويشمل الإدخال والإتلاف والمحو لمعطيات الكمبيوتر أو برامجه، أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى إلحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.

٢- تزوير الكمبيوتر أو التزوير المعلوماتي: ويشمل إدخال أو إتلاف أو محو أو تحويل المعطيات أو البرامج أو أية أفعال تؤثر على المجري الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد- فيما لو ارتكبت بغير هذه الطرق- من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.

٣- الإضرار بالبيانات والبرامج (الإتلاف): وتشمل المحو والاتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه.

٤- تخريب وإتلاف الكمبيوتر: وتشمل الإدخال أو المحو أو الإتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات (الشبكات).

٥- الدخول غير المصرح به: وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن.

الاعتراض غير المصرح به، وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات.

## ثانيا: في الشق الإجرائي

قرار صادر عن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون

العقوبات حول القواعد الإجرائية في بيئة جرائم الكمبيوتر

١- يتطلب التنقيب Lenquete بالنسبة لجرائم الحاسب الآلي، والجرائم الأكثر تقليدية في بيئة تكنولوجيا المعلومات- لمصلحة الدفاع الاجتماعي الفعال- أن نضع تحت تصرف سلطات التحقيق instruction والتحري pour suite مكنات قسرية كافية تتعادل مع الحماية الكافية لحقوق الإنسان وحرمة الحياة الخاصة.

٢- لتجنب تعسف السلطات الرسمية، فإن القيود التي ترد علي حقوق الإنسان عن طريق رجال السلطة العامة، لا يمكن أن تكون مقبولة إلا في الحالة التي تكون فيها مرتكزة علي قواعد قانونية واضحة ودقيقة ومتماشية مع المعايير الدولية لحقوق الإنسان.

إن الانتهاكات غير المشروعة لحقوق الإنسان التي يرتكبها رجال السلطة العامة، يمكن أن تبطل الدليل المتحصل عليه، بالإضافة إلي تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون.

٣- علي ضوء هذه المبادئ العامة يجب أن يحدد بوضوح ما يلي:

أ- السلطات التي تقوم بإجراء التنقيش La perquisition والضبط La saisie في بيئة تكنولوجيا المعلومات، وخاصة ضبط الأشياء غير المحسوسة Biens non corporals وتفتيش شبكات الحاسب.

ب- واجبات التعاون الفعال من جانب المجني عليهم Victimes، والشهود Temoins، وغيرهم من مستخدمي utilisaterurs تكنولوجيا المعلومات، فيما خلا المشتبه suspect (خاصة لكي تكون المعلومات متاحة في صورة يمكن استخدامها للأغراض القضائية fins judiciaires).

ج- السماح للسلطات العامة باعتراض interception الاتصالات داخل نظام الحاسب ذاته، أو بينه وبين نظم الحاسبات الأخرى. مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم.

د- نظرا لتعدد وتنوع البيانات المدرجة في نظم معالجة البيانات des systems traitement inforatiique، فإن تنفيذ المكنات القسرية (المنوطة برجال السلطة العامة) يجب أن يكون متناسبا مع الطابع الخطير للانتهاك، ولا يسبب سوى الحد الأدنى من إعاقة genante الأنشطة القانونية للفرد. كما يجب عند بدء التحريات investigations أن يوضع في الاعتبار - بالإضافة إلى القيم المالية التقليدية- كل القيم المرتبطة ببيئة تكنولوجيا المعلومات، مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسارة الاقتصادية، كلفة Lecout إعادة بناء تكامل البيانات كما كانت من قبل.

هـ- القواعد القائمة في مجال قبول ومصادقية الأدلة، يمكن أن تثير مشاكل عند تطبيقها، نظرا لتقييم تسجيلات الحاسبات levaluation des enregistrements informatiques في الإجراءات القضائية لذا ينبغي إدخال بعض التغييرات التشريعية في حالة الضرورة.





**رابعاً**

**قرار بشأن الجرائم ذات**

**الصلة بالكمبيوتر**



## قرار بشأن الجرائم ذات الصلة بالكمبيوتر

إن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء إذ يسلم بضرورة تطوير سبل ووسائل التعاون في المسائل الجنائية، ورغبة منه في استكمال العمل الذي أنجز في ميدان معايير الأمم المتحدة وقواعدها في ميدان العدالة الجنائية.

وإذ يضع في اعتباره أن نظم الكمبيوتر كثيرا ما تستعمل لتخزين بيانات سياسية واقتصادية وطبية واجتماعية وشخصية تنتم بحساسة بالغة، وأن هذه النظم قد تستخدم لأداء ومراقبة مهام معقدة كثيرا ما تتطوي علي حالات قد تعرض للخطر الحياة وحقوق الإنسان والحريات الأساسية.

وإذ يدرك أن زيادة استخدام تكنولوجيا الكمبيوتر وشبكات الاتصالات السلكية واللاسلكية علي نطاق العالم عن طريق الكمبيوتر بوصفها جزءا لا يتجزأ من العمليات المالية والمصرفية الدولية قد تهيئ ظروفًا تيسر إلي حد كبير من ارتكاب العمليات الإجرامية داخل البلدان وفيما بينها.

وإذ يساوره القلق لزيادة إساءة استعمال الكمبيوتر كإحدى طرق الجريمة الاقتصادية وصعوبة الكشف عن الجرائم ذات الصلة بالكمبيوتر، وخصوصا بسبب السرعة التي يمكن أن ترتكب بها هذه الجرائم.

وإذ يساوره القلق أيضا لزيادة النفاذ غير المصرح به إلي نظام الكمبيوتر وبياناته وبرامجه والإقدام دون إذن علي استعمالها أو مراقبتها، أو التدخل فيها، أو ارتكاب أفعال ضارة أخرى ذات صلة بنظمه وبياناته وبرامجه.

وإذ يلاحظ إمكانية الربط بين الجريمة المنظمة ومال يتصل بها من إساءة استعمال الكمبيوتر وأن الكمبيوتر كثيرا ما قد تستخدمه الجريمة المنظمة لأغراض من قبيل غسل الأموال أو في إدارة الأصول المتحصلة بطريقة غير مشروعة.

وإذ يأخذ في اعتباره أيضا أعمال منظمة التعاون الاقتصادي والتنمية ولا سيما تقريرها الصادر عام ١٩٨٦ وتوصية وتقرير مجلس أوروبا بشأن الجرائم المتعلقة بالكمبيوتر والمبادئ التوجيهية التشريعية التي اعتمدتها اللجنة الوزارية لمجلس أوروبا في ١٣ أيلول/سبتمبر ١٩٨٩.

وإذ يأخذ في اعتباره كذلك مشروع المبادئ التوجيهية المتعلقة باستعمال ملفات البيانات الشخصية في نظم الكمبيوتر المعد من قبل اللجنة الفرعية لمنع التمييز وحماية الأقليات.

وإذ يضع في اعتباره أن عددا من الدول الأعضاء تضطلع منذ مدة بشأن المسائل المتعلقة بالجرائم المتصلة بالكمبيوتر بما في ذلك إعداد دراسات وبحوث وسن تشريعات.

وإذ يسلم بضرورة مواصلة العمل من أجل التوصل إلى توافق دولي في الآراء بشأن أنماط إساءة استخدام الكمبيوتر التي يتعين اعتبارها سلوكا إجراميا.

واقترعا منه بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية ديناميكية في ضوء الطابع الدولي والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به.

فإنه:

١- يؤكد أن وضع إجراء دولي ملائم يتطلب بذل جميع الدول الأعضاء جهدا جماعيا.

٢- يهيب بالدول الأعضاء، في ضوء الأعمال المطروح بها فعلا في مجال الجرائم ذات الصلة بالكمبيوتر أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة استعمال الكمبيوتر التي تستدعي تطبيق إجراءات جنائية علي الصعيد الوطني بما في ذلك النظر، إذا دعت الضرورة إلى ذلك، في التدابير التالية:

أ- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل:

- ١- ضمان أن تطبق الجزاءات والقوانين الراهنة، بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية علي نحو ملائم وإدخال تغييرات مناسبة إذا دعت الضرورة إلي ذلك.
- ٢- وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة. للتصدي إلي هذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي.
- ٣- مصادرة أو رد الأصول بصورة غير مشروعة والناجمة عن ارتكاب جرائم ذات صلة بالحاسوب.
- ب- تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة حماية الخصوصية واحترام حقوق الإنسان وحياته الأساسية.
- ج- اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة إنفاذ القوانين بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحوسيب.
- د- اعتماد تدابير مناسبة لتدريب القضاة والمسؤولين والأجهزة المسؤولة عن منع الجرائم الاقتصادية والجرائم ذات الصلة بأجهزة الحاسوب والتحقيق فيها ومحاكمة مرتكبيها وإصدار الأحكام المتعلقة بها.
- هـ- التعاون مع المنظمات المتهممة بهذا الموضوع في وضع قواعد للآداب المتبعة في استخدام أجهزة الحاسوب وتدريب هذه الآداب ضمن المناهج الدراسية.
- و- اعتماد سياسات بشأن ضحايا الجرائم المتعلقة بالكمبيوتر تتسجم مع إعلان الأمم المتحدة بشأن مبادئ العدل المتعلقة بضحايا الإجمام والتعسف في استعمال السلطة، وتتضمن إعادة الممتلكات التي يتم الحصول عليها بطرق غير مشروعة، وتدابير لتشجيع الضحايا علي إبلاغ السلطات المختصة بهذه الجرائم<sup>(١)</sup>.

(١) ثمة جزء إضافية من القرار يركز علي أهمية التعاون الدولي في ميدان مكافحة واتخاذ التدابير التشريعية والكفيلة بالمشاركة في معاهدات وترتيبات تسليم المجرمين والتعاون في أعمال التحقيق بين الدول إضافة إلي تكليف الأمين العام للأمم المتحدة والدول الأعضاء بتوفير ميزانيات أنشطة مكافحة.



**خامسا**

**الإعلان الخامس باستخدام التقدم**

**العلمي والتكنولوجي**

**لصالح السلم وخير البشرية**





## الإعلان الخاص باستخدام التقدم

### العلمي والتكنولوجي لصالح السلم وخير البشرية

إن الجمعية العامة:

إذ تلاحظ أن التقدم العلمي والتكنولوجي قد أصبح أحد أهم العوامل في تطور المجتمع الإنساني،

وإذ تضع في اعتبارها أن التطورات العلمية والتكنولوجية، علي كونها تتيح باستمرار فرصاً متزايدة لتحسين أحوال معيشة الشعوب والأمم، يمكن أن تولد في عدد من الحالات مشاكل اجتماعية، وأن تهدد كذلك ما للفرد من حقوق الإنسان والحريات الأساسية.

وإذ تُري مع القلق أن المنجزات العلمية والتكنولوجية يمكن أن تستخدم لزيادة حدة سباق التسلح، وقمع حركات التحرر الوطني، وحرمان الأفراد والشعوب من حقوقهم الإنسانية وحرياتهم الأساسية،

وإذ تُري أيضاً مع القلق أن المنجزات العلمية والتكنولوجية يمكن أن تعرض للأخطار الحقوق المدنية السياسية للفرد أو للجماعة، والكرامة البشرية.

وإذ تلاحظ الحاجة الملحة إلي الاستفادة كليا من التطورات العلمية والتكنولوجية من أجل رفاهية الإنسان ولإبطال مفعول الآثار الضارة المترتبة حالياً أو التي يمكن أن تتربط في المستقبل علي بعض المنجزات العلمية والتكنولوجية،

ومع اعترافها بأن التقدم العلمي والتكنولوجي ذو شأن بالغ الأهمية في التعجيل بالإنماء الاجتماعي والاقتصادي للبلدان النامية، ولما كانت علي بيئة من أن نقل العلم والتكنولوجيا هو أحد السبل الأساسية للتعجيل بالإنماء الاقتصادي للبلدان النامية، وإذ تؤكد من جديد حق الشعوب في تقرير المصير

وضرورة احترام حقوق الإنسان وحياته وكرامة الشخص البشري في ظروف التقدم العلمي والتكنولوجي.

ورغبة منها في تعزيز تحقيق المبادئ التي تشكل أساس ميثاق الأمم المتحدة، والإعلان العالمي لحقوق الإنسان، والعهد الدولي الخاصين بحقوق الإنسان، وإعلان منح الاستقلال للبلدان والشعوب المستعمرة، وإعلان مبادئ القانون الدولي معلقة بالعلاقات الودية والتعاون بين الدول وفقاً لميثاق الأمم المتحدة، وإعلان التقدم والإنماء في الميدان الاجتماعي، وميثاق حقوق الدول وواجباتها الاقتصادية، تعلن رسمياً ما يلي:

١- علي جميع الدول أن تنهض بالتعاون الدولي لضمان استخدام نتائج التطورات العلمية والتكنولوجية لصالح تدعيم السلم والأمن الدوليين، والحرية والاستقلال، وكذلك لغرض الإنماء الاقتصادي والاجتماعي للشعوب وأعمال حقوق الإنسان وحياته وفقاً لميثاق الأمم المتحدة.

٢- علي جميع الدول أن تتخذ تدابير ملائمة لمنع استخدام التطورات العلمية والتكنولوجية، ولا سيما من جانب الهيئات التابعة للدولة، للحد من تمتع الفرد بما له من حقوق الإنسان والحريات الأساسية، كما هي مكرسة في الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاصين بحقوق الإنسان والصكوك الدولية الأخرى ذات الصلة بالموضوع، أو لعرقلة هذا التمتع.

٣- علي جميع الدول أن تتخذ تدابير لكفالة جعل المنجزات العلمية والتكنولوجية تلبي الحاجات المادية والروحية لجميع قطاعات السكان.

٤- علي جميع الدول أن تمتنع عن أية أعمال تستخدم فيها المنجزات العلمية والتكنولوجية لأغراض انتهاك سيادة الدول الأخرى وسلامتها الإقليمية، أو للتدخل في شئونها الداخلية، أو شن الحروب العدوانية، أو قمع

حركات التحرير لوطني أو تنفيذ سياسة قائمة علي التمييز العنصري. فهذه الأعمال لا تمثل خرقا صارخا لميثاق الأمم المتحدة ومبادئ القانون الدولي فحسب، بل تشكل أيضا تشويها غير مقبول للمقاصد التي ينبغي أن توجه للتطورات العلمية والتكنولوجية لخير البشرية.

٥- علي جميع الدول أن توازر في إقامة القدرات العلمية والتكنولوجية للبلدان النامية وتعزيزها وتنميتها بغية تعجيل أعمال الحقوق الاجتماعية والاقتصادية لشعوب تلك البلدان.

٦- علي جميع الدول أن تتخذ تدابير تهدف إلي تمكين جميع طبقات السكان من الإفادة من حسنات العلم والتكنولوجيا وإلي حماية هذه الطبقات، لاجتماعيا، وماديا، من الآثار الضارة التي يمكن أن تترتب علي سوء استخدام التطورات العلمية والتكنولوجية، بما في ذلك إساءة استعمالها علي نحو يمس بحقوق الفرد أو الجماعة، ولا سيما فيما يتعلق باحترام الحياة الخاصة وحماية شخصية الإنسان وسلامته البدنية والذهنية.

٧- علي جميع الدول أن تتخذ تدابير فعالة، بما في ذلك التدابير التشريعية، لكفالة جعل المنجزات العلمية والتكنولوجية تستخدم لتأمين الأعمال الأكمل لحقوق الإنسان والحريات الأساسية دون أي تمييز بسبب العنصر أو الجنس أو اللغة أو المعتقدات الدينية.

٨- علي جميع الدول أن تتخذ تدابير فعالة، بما في ذلك التدابير التشريعية لمنع وتلاقي استخدام المنجزات العلمية والتكنولوجية للإضرار بحقوق الإنسان والحريات الأساسية وبكرامة الشخص البشري.

٩- علي جميع الدول أن تتخذ، كلما اقتضى الأمر، إجراءات تستهدف كفالة الامتثال للتشريعات التي تضمن حقوق الإنسان وحرياته علي ضوء التطورات العلمية والتكنولوجية.

حضر مرحلة جنيف من القمة العالمية وفود رفيعة المستوى من ١٧٥ بلدا تشمل رئيس ونائب رئيس ٥٠ دولة وحكومة. وشارك أكثر من ١١٠٠... شخص في القمة العالمية والأنشطة المتصلة بالقمة.

واعتمد زعماء العالم المجتمعين في مرحلة جنيف من القمة العالمية في ١٢ ديسمبر ٢٠٠٣ إعلان مبادئ القمة وعنوانه "بناء مجتمع المعلومات: تحد عالمي في الألفية الجديدة". وهذا الإعلان يضع أسس مجتمع المعلومات الناشئ.

وتضع خطة عمل القمة التي أيدتها قمة جنيف أهدافا مرتبطة بمواعيد زمنية لترجمة المعلومات الجامع والمنصف من رؤية إلي واقع عملي.

التقرير النهائي لمرحلة جنيف من القمة العالمية.

اعتمد المجتمع المدني "إعلان المجتمع المدني" الذي تضمن مدخلات مقدمة إلي القمة العالمية.

#### لماذا هناك حاجة لعقد مؤتمر قمة عالمي لمجتمع المعلومات؟

هناك تحول جذري يحدث من المجتمع الصناعي إلي المجتمع القائم علي المعلومات. وتؤثر تلك الثورة المعلوماتية علي الطريقة التي يعيش بها الناس، ويتعلمون ويعملون، وعلي الطريقة التي تتفاعل بها الحكومات مع المجتمع المدني. وتعد المعلومات أداة قوية لتحقيق التنمية الاقتصادية والاجتماعية، وسوف توفر تلك القمة فرصة فريدة لجميع العناصر الفاعلة الأساسية للإسهام بشكل إيجابي في تجسير الهوة الرقمية وهوة المعرفة. وسوف تقرر المرحلة الأولى للقمة في جنيف إعلانا للمبادئ وخطة للعمل لتضعها الحكومات، والمؤسسات، وجميع قطاعات المجتمع المدني موضع التنفيذ للتعامل مع التحديات الجديدة لمجتمع المعلومات دائم التطور، وخصوصا التعرف علي الطرق التي من شأنها المساعدة علي سد الهوة بين الأغنياء والفقراء من حيث الوصول إلي المعلومات العالمية وشبكات الاتصال.

وستكون محاور التنمية موضوعا أساسيا تركز عليه المرحلة الثانية بتونس العاصمة، وستقوم بتقييم التقدم الذي تم إحرازه، وإقرار أية خطة عمل إضافية يجدر اتخاذها.

#### ما المقصود تحديدا بالانقسامات الرقمية والانقسامات في المعرفة؟

يشير هذان المصطلحان إلى الهوة القائمة بين المجتمعات التي تمكنها التكنولوجيا والمجتمعات التي تستبعد التكنولوجيا علي كوكبنا، إضافة إلى قلة سبل نقل المعلومات داخل تلك المجتمعات وبين بعضها البعض. ويشمل العالم النامي والاقتصاديات التي تمر بمرحلة انتقالية أكبر نسبة من الانقسامات الرقمية والانقسامات في المعارف. وبينما تبين كثافة الخطوط الهاتفية علي مستوى العالم بعض علامات التحسن - حيث تخطي عدد الخطوط الهاتفية بالنسبة لكل مائة شخص الشخص الواحد عام ٢٠٠١ - فإن الهوة بين الذين يتمتعون بالوصول إلى الإنترنت والذين لا يتمتعون به، من ناحية أخرى، تستمر في الاتساع في كافة أنحاء العالم.

#### هل يغير مجتمع المعلومات حياتنا؟

ظهر بيننا اقتصاد جديد نتصل أركانه ببعضها البعض عن طريق شبكات، كما ظهر مجتمع معلومات يقوم علي المعرفة. وقد تغيرت الطريقة التي يعيش بها الأشخاص، ويتعلمون، ويعلمون، ويتفاعلون مع بعضهم البعض بصورة لا يمكن إعادتها إلى سابق عهدها.

#### ما العلاقة بين مجتمعات المعلومات والمعارف؟

كان للتنفق الحر للمعلومات والأفكار الفضل في نمو متفجر في المعارف ومآلها من تطبيقات جديدة لا عد لها ولا حصر، وكنتيجة لذلك، تم تحويل الهياكل والعلاقات الاقتصادية والاجتماعية. إلا أنه تظل الغالبية العظمي من الأشخاص في العالم بمنأى عن تلك الثورة. فيهدد ذلك "الانقسام الرقمي"

بتوسيع هوة التنمية القائمة بالفعل بين الأغنياء والفقراء، سواء علي مستوى البلدان المختلفة أو داخل حدود البلد الواحد. ولن يتمكن غالبية الأشخاص بالعالم من جني ثمار تلك الثورة، ما لم يتم تمكينهم من المشاركة الكاملة في مجتمع المعلومات الناشئ والقائم علي المعرفة.

#### كيف يدفع مجتمع المعلومات بعجلة الاقتصاديات؟

تؤدي الثورة الرقمية إلي نشوء أفكار جديدة تماما من التفاعل الاجتماعي والاقتصادي وقيام مجتمعات جديدة داخل فضاء سبراني. وعلي عكس الثورة الصناعية التي شهدتها القرن المنصرم، فإن ثورة تكنولوجيا المعلومات والاتصال من شأنها الانتشار بشكل سريع والتأثير في حية الجميع. وتتمحور تلك الثورة قوة تكنولوجيا المعلومات والاتصالات التي تسمح للناس بالوصول إلي المعلومات والمعرفة الموجودة في أي مكان بالعالم في نفس اللحظة تقريبا.

#### ما الدور الذي يمكن لتكنولوجيا المعلومات والاتصال أن تلعبه في التنمية الاقتصادية والاجتماعية؟

خلق "الانقسام الرقمي" فجوة في المعارف بين الشعوب الغنية بالمعلومات وتلك التي تفتقر إليها، مما قد يمهد السبيل لظهور أشكال جديدة من "الأمية". ويعزز الانقسام الرقمي الافتقار إلي المعلومات والمعرفة، ويحدد فرص النمو الاقتصادي وتوزيع الثروة. وتشجع تكنولوجيا المعلومات والاتصال علي إقامة "شبكات" اقتصادية واجتماعية من الأفراد والمجتمعات. تتمثل قوة تلك الشبكات في قدرتها علي الربط بين المجموعات المتنوعة عن طريق السماح لها بالوصول إلي المعلومات والمعارف الجوهرية لتحقيق تنميتها الاقتصادية الاجتماعية وتبادل تلك المعلومات والمعارف. ويستفيد التجار وأصحاب الأعمال والمشروعات من تكنولوجيا المعلومات والاتصال من خلال الفرص التي تهيئها عن طريق النهوض بأعمالهم وطنيا وإقليميا ودوليا. وعلاوة علي

ما تقدم، فإن تكنولوجيا المعلومات والاتصال تتيح الفرصة لتقديم الخدمات الأساسية في مجال الصحة والتعليم علي نحو أكثر كفاءة، حيث يمكن للناس الوصول إليها من داخل مجتمعاتهم.

**ما هو العهد الذي قطعه مجتمع المعلومات علي نفسه؟**

زيادة قدرتنا علي الاتصال وتقاسم المعلومات والمعارف يرفع من فرصة تحول العالم إلي مكان أكثر سلماً ورخاء لجميع سكانه. بيد أن غالبية الأشخاص بالعالم لن يتمكنوا من جني ثمار المعلومات هذه، ما لم يتم تمكينهم من المشاركة الكاملة في مجتمع المعلومات الناشئ والقائم علي المعرفة.

**من الذي يجب أن يتمتع بحق الوصول؟**

لابد أن يسهل الوصول إلي المعارف والمعلومات علي الجميع، بما في ذلك الذين يعيشون في المناطق الريفية والمعاقين. ولابد من إيلاء الاهتمام الخاص بالمهمشين، والعاطلين عن العمل، والمعدمين، والشعور المحرومة من حقوقها، والأطفال، وكبار السن، والمعاقين، وجماعات السكان الفطريين، وذوي الاحتياجات الخاصة.

**ما هي القيم التي ينبغي أن تقوم علي أسس مجتمع المعلومات؟**

تعتبر القيم الإنسانية العالمية، المتمثلة في المساواة، والعدالة، والديموقراطية، والتضامن والتسامح المتبادل، والكرامة الإنسانية، والتقدم الاقتصادي، وحماية البيئة، واحترام التنوع أسس لمجتمع معلومات عالمي يكون شاملاً بمعنى الكلمة.

**هل سيقر مؤتمر القمة العالمي لمجتمع المعلومات نصاً يوفر رؤية عالمية لمجتمع المعلومات؟**

سوف يتيح مؤتمر القمة العالمي فرصة فريدة لجميع العناصر الفاعلة الرئيسية لوضع رؤية مشتركة وتحقيق فهم أفضل لمجتمع المعلومات،

ووضع خطة عمل استراتيجية من أجل إعمال تلك الرؤية لما فيه مصلحة البشرية قاطبة.

#### ما القضايا التي سيتم وضعها في الاعتبار؟

توفر الوثيقة العاملة لخطة العمل قائمة بالقضايا التي سيتم استخدامها كإطار مرجعي تتضمن تلك القضايا:

١- البنية التحتية للمعلومات والاتصالات: التمويل والاستثمار، وسهولة المنال، والتطور، والاستدامة.

٢- الوصول إلى المعلومات والمعرفة.

٣- دور الحكومات، وقطاع الأعمال، والمجتمع المدني في تعزيز تكنولوجيات المعلومات والاتصال من أجل التنمية.

٤- بناء القدرة: تنمية الموارد البشرية، والتعليم والتدريب.

٥- الأمن.

٦- البيئة المواتية.

٧- النهوض بتطبيقات تكنولوجيا المعلومات والاتصال الموجهة نحو التنمية للجميع.

٨- الهوية الثقافية والتنوع اللغوي، والمحتوي المحلي، والتطور الإعلامي.

٩- تحديد العوائق والتغلب عليها من أجل تحقيق مجتمع معلومات له منظوره الإنساني.

#### لماذا تعد البنية التحتية والتمويل أمورا هامة؟

يمكن لتكنولوجيا المعلومات والاتصال الإسهام بصورة قوية في تحقيق التنمية الاقتصادية والاجتماعية والنمو المستدام بجميع البلدان. إلا أن نقص



البنية الأساسية والموصولية في غالبية البلدان النامية يظل تحديا يحول دون تنمية مجتمع المعلومات. ومن أجل الاستفادة من الفرص التي تتيحها تكنولوجيا المعلومات والاتصال من أجل التنمية والرخاء، يمكن من الضروري أن تتحقق للبشرية جنعاء سبل الوصول إليها. ولهذا السبب، تتجلى الأهمية الجوهرية لإقامة نقاط وصول عامة في كل مجتمع، وتوفير معدات للوصول تكون منخفضة التكلفة ، فضلا عن تحقيق الترابط.

لماذا تعد اتفاقيات الشراكة بين القطاع العام، والقطاع الخاص، والمجتمع المدني مهمة في تعزيز تكنولوجيا المعلومات والاتصال من أجل التنمية؟

لابد من إرساء دعائم اتفاقيات للشراكة يكون مرامها تحقيق الأهداف المشتركة والتعامل مع القضايا ذات الصلة بتكنولوجيا المعلومات والاتصال. فلا بد للقطاع العام من بحث السبل التي يمكن من خلالها تصويب إخفاقات السوق، وتشجيع المنافسة من أجل توصيل مجتمع المعلومات للجميع، لا سيما في البلدان النامية. وللقطاع الخاص دور هام يلعبه في الاستثمار في تكنولوجيا المعلومات والاتصال، ويتعين علي الحكومات تشجيع مشاركته. ولابد من عمل المجتمع المدني فسي تعاون وثيق مع المجتمعات من أجل تقوية مبادرات تكنولوجيا المعلومات والاتصال. كما ينبغي علي المنظمات الدولية المساعدة علي إيماج تكنولوجيا المعلومات والاتصال في عملية التنمية، بالإضافة إلي دعم تنفيذ أهداف خطة عمل مؤتمر القمة العالمي لمجتمع المعلومات.

لماذا تعد تنمية الموارد البشرية، والتعليم، والتدريب، أمور ذات صلة بإقامة مجتمع شامل للمعلومات؟

من أجل الاستفادة بشكل كامل من مجتمع المعلومات، فمن الضرورة بمكان أن يرتفع مستوى مهارات تكنولوجيا المعلومات والاتصال. ولهذا

السبب، فلابد من توفير التعليم والتدريب ذي الصلة علي كافة المستويات، خاصة بالنسبة للشباب. وتتمثل الحاجة إلي استراتيجيات التعليم الإلكتروني من أجل الوصول إلي هؤلاء دون النفاذ إلي النظام التعليمي الرسمي بسبب الجغرافيا أو الظروف الشخصية.

#### **لماذا يعد الأمن قضية جديرة بالاهتمام بالنسبة لمجتمع المعلومات؟**

تعد قضية الأمن قضية جوهرية في تنمية مجتمع المعلومات، حيث تفرض الجرائم السيبرانية، مثل القرصنة، وانتشار فيروسات الكمبيوتر، وإساءة استخدام المعلومات الشخصية تهديدات خطيرة للاقتصاديات القائمة علي المعلومات. وبزيادة الأعمال الإلكترونية والصفقات التي تتم عن طريق الإنترنت، تكون حماية الخصوصية وضمان وجود بنية تحتية آمنة لتكنولوجيا المعلومات والاتصال عناصر هامة لإقامة مجتمع مستقر للمعلومات.

#### **ماذا نعني "بالبيئة المواتية"؟**

أدي ظهور تحديات قانونية ترتبط باستخدام وسوء استخدام بيانات تكنولوجيا المعلومات والاتصال إلي الحاجة لوجود أطر ملائمة، قانونية وتنظيمية وأخرى تتصل بالسياسات، علي المستويات العالمية، والإقليمية، والوطنية. ولابد لتلك الأطر أن تضع نصب أعينها حقوق الجميع والتزاماتهم بالنسبة لحرية التعبير، والخصوصية، والأمن، وحقوق الملكية الفكرية، وإدارة عناوين الإنترنت وأسماء النطاقات، وحماية المستهلك.

#### **ما هو نوع تطبيقات تكنولوجيا المعلومات والاتصال المواجهة نحو التنمية التي يمكن تصورها؟**

سمحت تكنولوجيا المعلومات والاتصال بقيام سوق عالمية يمكن فيها الوصول إلي كم كبير من المعلومات، والسلع، والخدمات، وتتيح تكنولوجيا المعلومات والاتصال فرصا عديدة للبلدان النامية للتعجيل بتنميتها الاجتماعية

والاقتصادية. وتتضمن تطبيقات تكنولوجيا المعلومات والاتصال الموجهة نحو التنمية الحكومة الإلكترونية (لتحسين الخدمات العامة)، والأعمال الإلكترونية، والتعليم الإلكتروني، والصحة الإلكترونية.

هل ستهيمن لغة أو ثقافة واحدة علي مجتمع المعلومات؟

إن وضع محتوى متعدد اللغات لجميع أشكال تكنولوجيا المعلومات والاتصال هو أمر لا بد من النهوض به لضمان الحفاظ علي التنوع الثقافي المحلي والوطني، واللغة، والتراث، والمعارف والتقاليد الفطرية.

هل سيتم احترام حرية التعبير؟

تنص المادة التاسعة عشرة من إعلان الأمم المتحدة العالمي لحقوق الإنسان علي أنه لكل شخص الحق في حرية الرأي والتعبير. ويشمل هذا الحق حرية اعتناق الآراء دون أي تدخل، واستقاء الأنباء والأفكار وتلقيها وإذاعتها بأية وسيلة كانت دون تقيد بالحدود الجغرافية. وستراعي القمة الحفاظ علي هذا الحق.

ما هو الدور الذي يمكن لتكنولوجيا المعلومات والاتصال، بالإضافة إلي وسائل الإعلام التقليدية والحديثة، أن تلعبه، في أعمال إدارة تكون أكثر كفاءة؟

تمكن تكنولوجيا المعلومات والاتصال، بالإضافة إلي وسائل الإعلام التقليدية والحديثة، الأشخاص المهمشين والمعزولين من أن يملوا بملوهم في المجتمع العالمي، بغض النظر عن نوعهم أو مكان سكنهم. وهي تساعد علي التسوية بين القوة وعلاقات صنع القرار علي المستويين المحلي والدولي. ويوسعها تمكن الأفراد، والمجتمعات، والبلدان من تحسين مستوى حياتهم علي نحو لم يكن ممكناً في السابق. ويمكنها أيضاً المساعدة علي تحسين كفاءة الأدوات الأساسية للاقتصاد الديمقراطي من خلال الوصول إلي المعلومات والشفافية.



سادسا

القمة العالمية لاجتمع المعلومات



## مشروع إعلان المبادئ

### ألف - رؤيتنا المشتركة لمجتمع المعلومات

١- نحن ممثلو شعوب العالم وقد اجتمعنا في جنيف من ١٠ إلى ١٢ ديسمبر ٢٠٠٣ للمرحلة الأولى من القمة العالمية لمجتمع المعلومات، نعلن رغبتنا المشتركة والتزامنا المشترك لبناء مجتمع معلومات جامع غايته الناس ويترجمه نحو التنمية، مجتمع يستطيع كل فرد فيه استحداث المعلومات والمعارف والنفاذ إليها واستخدامها وتقاسمها، بحيث يمكن الأفراد والمجتمع والشعوب من تسخير كامل إمكاناتهم في النهوض بتنميتهم المستدامة وفي تحسين نوعية حياتهم، وذلك انطلاقاً من مقاصد ومبادئ ميثاق الأمم المتحدة وإيلاء الاحترام الكامل والتأييد للإعلان العالمي لحقوق الإنسان.

٢- والتحديات الذي نتصدي له هو تسخير إمكانات تكنولوجيا المعلومات والاتصالات للنهوض بأهداف التنمية الواردة في إعلان الألفية، وهي استئصال الفقر المدقع والجوع؛ وتحقيق التعليم الابتدائي للجميع؛ وتعزيز المساواة بين الجنسين وتمكين المرأة؛ خفض معدلات وفيات الأطفال؛ وتحسين صحة الأمهات؛ ومكافحة فيروس نقص المناعة البشرية/ الإيدز والملاريا وغيرهما من الأمراض؛ وضمان الاستدامة البيئية؛ وإقامة شراكة عالمية من أجل التنمية وذلك سعياً لزيادة السلم والعدل والرخاء في العالم. ونحن نؤكد من جديد التزامنا بتحقيق التنمية المستدامة وأهداف التنمية المتفق عليها، على نحو ما جاء في إعلان جوهانسبرغ وخطة التنفيذ وتوافق آراء مونترالي، وغيرها من نواتج مؤتمرات القمة التي عقدتها الأمم المتحدة في هذا الصدد.

٣- ونؤكد من جديد عالمية كل حقوق الإنسان والحريات الأساسية وعدم قابليتها للتجزئة والترابط فيما بينها، بما في ذلك الحق في التنمية، المنصوص عليه في إعلان فيينا. ونؤكد من جديد أيضاً أن الديمقراطية والتنمية

المستدامة واحترام حقوق الإنسان والحريات الأساسية وكذلك الحكم الرشيد علي جميع المستويات يعتمد بعضها علي بعض ويعزز بعضها بعضا. ونقرر كذلك تعزيز احترام سيادة القانون في الشؤون الدولية كما في الشؤون الوطنية.

٤- ونؤكد من جديد، كأساس جوهري لمجتمع المعلومات وكما ورد في المادة ١٩ من الإعلان العالمي لحقوق الإنسان، أن لكل فرد الحق في حرية الرأي والتعبير؛ وأن هذا الحق يشمل حرية اعتناق الآراء دون أن تدخل، واستبقاء الأنباء والأفكار وتلقيها وإذاعتها بأية وسيلة كانت دون تقيد بالحدود الجغرافية. والاتصال عملية اجتماعية أساسية، وحاجة إنسانية أساسية، وهو أساس كل تنظيم اجتماعي. وهو محور مجتمع المعلومات. وينبغي لكل فرد في كل مكان أن تتاح له الفرصة للمشاركة، ولا ينبغي استبعاد أحد من الفوائد التي يقدمها مجتمع المعلومات.

٥- ونؤكد من جديد كذلك التزامنا بأحكام المادة ٢٩ من الإعلان العالمي لحقوق الإنسان، وأن علي كل فرد واجبات نحو المجتمع الذي يتاح فيه وحده لشخصيته أن تنمو نموذجا حرا كاملا، وأن الفرد يخضع في ممارسته حقوقه وحرياته لتلك القيود التي يقرها القانون فقط لضمان الاعتراف بحقوق الغير وحرياته واحترامها ولتحقيق المقتضيات العادلة للنظام العام والمصلحة العامة والأخلاق في مجتمع ديمقراطي. ويجب ألا تمارس هذه الحقوق والحريات البتة بما يخالف مقاصد ومبادئ الأمم المتحدة. وبهذا الشكل سنعمل علي النهوض بمجتمع للمعلومات نحترم فيه كرامة البشر.

٦- وتمشيا مع روح هذا الإعلان فإننا نجدد تعهدنا بدعم مبدأ المساواة في السيادة بين جميع الدول.

٧- ونقر بأن العلوم لها دور مركزي في تطوير مجتمع المعلومات. فالكثير من العناصر المساهمة في بناء مجتمع المعلومات إنما هي حصيلة خطوات التقدم العلمي والتقني التي تحققت بفضل تبادل نتائج البحوث.



٨- ونعترف بأن التعليم والمعرفة والمعلومات والاتصالات هي بؤرة تقدم البشرية ومساعدتها ورفاهها. وعلاوة على ذلك فإن تكنولوجيا المعلومات والاتصالات تؤثر تأثيراً هائلاً على جميع مظاهر الحياة تقريباً. كما أن سرعة تقدم هذه التكنولوجيات تكشف عن فرص جديدة كلياً لبلوغ مستويات أرفع من التنمية. وقدرة هذه التكنولوجيات على تذليل العديد من العقبات التقليدية، وخصوصاً ما يتعلق باختصار الزمن والمسافات، تجعل من الممكن ولأول مرة في التاريخ تسخير إمكانات هذه التكنولوجيات لصالح الملايين من الناس في جميع أرجاء المعمورة.

٩- ونذكر أن تكنولوجيا المعلومات والاتصالات ينبغي أن تستخدم كأدوات وليس كغاية بحد ذاتها. وفي الظروف المؤاتية يمكن أن تكون هذه التكنولوجيات وسيلة جبارة تزيد الإنتاجية وتولد النمو الاقتصادي وتدعم خلق فرص العمل وإمكانية الاستخدام وتحسين نوعية الحياة للجميع. وبمقدورها أيضاً تعزيز الحوار بين الناس والأمم والحضارات.

١٠- ونذكر أيضاً تمام الإدراك أن منافع ثورة تكنولوجيا المعلومات ليست موزعة توزيعاً متساوياً في الوقت الحاضر سواء بين البلدان المتقدمة والبلدان النامية أو في داخل المجتمعات. ونحن ملتزمون كل الالتزام بتحويل هذه الفجوة الرقمية إلى فرصة رقمية في متناول الجميع، وخصوصاً في متناول أولئك المعرضين للتخلف عن الركب ولمزيد من التهميش.

١١- ونحن ملتزمون بتحقيق رؤيتنا المشتركة لمجتمع المعلومات للجيل الحاضر وللأجيال المقبلة. وإننا ندرك أن الشباب هم القوى العاملة في المستقبل وأنهم في طليعة مبتكري تكنولوجيا المعلومات والاتصالات ومن أوائل الذين يبادرون إلى اعتناقها. ولذلك يجب تمكينهم كدارسين ومطورين ومساهمين وأرباب مشاريع وصانعي قرارات. ويجب أن نركز تركيزاً خاصاً على الشباب الذين نلم يتمكنوا بعد من الاستفادة كاملاً من الفرص

الممتاحة بفضل تكنولوجيا المعلومات والاتصالات. ونحن ملتزمون أيضا بكفالة احترام حقوق الطفل وضمان حمايته ورفاهه في سياق تطوير تكنولوجيا المعلومات والاتصالات وتشغيل خدماتها.

١٢- ونؤكد أن تطوير تكنولوجيا المعلومات والاتصالات يوفر فرصا هائلة للمرأة التي ينبغي أن تكون جزءا لا يتجزأ من مجتمع المعلومات وعنصرا فاعلا رئيسيا فيه. ونحن ملتزمون بالعمل على أن يتيح مجتمع المعلومات تمكين المرأة ومشاركتها الكاملة على أساس المساواة في جميع مجالات المجتمع وفي جميع عمليات صنع القرارات. وتحقيقا لذلك ينبغي لنا تعميم منظور المساواة بين الجنسين في كل مجال واستخدام تكنولوجيا المعلومات والاتصالات مطية لبلوغ هذه الغاية.

١٣- ولدى بناء مجتمع المعلومات سوف نخص بالاهتمام الاحتياجات الخاصة لدى الفئات المهمشة والضعيفة في المجتمع، بمن فيهم المهاجرون والأشخاص المشردون داخليا واللاجئون، والعاطلون عن العمل والمحرومين، والأقليات والجماعات الرحل. ولسوف نراعي أيضا الاحتياجات الخاصة لدى كبار السن ولدى الأفراد المعوقين.

١٤- ونحن مصممون تصميميا راسخا على تمكين الفقراء، وخاصة منهم الذين يعيشون في المناطق النائية والريفية وفي المناطق الحضرية المهمشة، من النفاذ إلى المعلومات واستخدام تكنولوجيا المعلومات والاتصالات كوسيلة لدعم جهودهم للخلاص من براثن الفقر.

١٥- وفي إطار تطور مجتمع المعلومات، يجب توجيه اهتمام خاص إلى الأوضاع الخاصة للشعوب الأصلية والعمل على صوت تراثهم ولوثهم الثقافي.

١٦- ونواصل توجيه اهتمام خاص إلى الاحتياجات التي تتفرد بها شعوب البلدان النامية والبلدان النامية غير الساحلية والبلدان الفقيرة المثقلة

بالديون والبلدان والأقاليم الخاضعة للاحتلال والبلدان الخارجة من الصراعات والبلدان والمناطق ذات الاحتياجات الخاصة وكذلك الظروف التي تثير تهديدات خطيرة للتنمية، كالكوارث الطبيعية.

١٧- ونقر بأن بناء مجتمع معلومات جامع يتطلب أشكالاً جديدة من التضامن والشراسة والتعاون بين الحكومات وأصحاب المصلحة الآخرين، أي القطاع الخاص والمجتمع المدني والمنظمات الدولية. وإذ ندرك أن بلوغ الهدف الطموح الذي يصبو إليه هذا الإعلان - إلا وهو سد الفجوة الرقمية وتحقيق تنمية متسقة وعادلة ومنصفة للجميع - سوف يتطلب التزاماً قوياً من جميع أصحاب المصلحة، فإننا ندعو إلى التضامن الرقمي، علي الصعيدين الوطني والدولي علي السواء.

١٨- ليس في هذا الإعلان ما يجوز تفسيره علي أنه ينتقص من أحكام ميثاق الأمم المتحدة والإعلان العالم لحقوق الإنسان أو من أي صك دولي آخر أو قوانين وطنية اعتمدت من أجل تعزيز هذين الصكين، أو يتناقض معها أو يقيدهما أو يبطلهما.

### **باء - مجتمع معلومات للجميع: مبادئ أساسية**

١٩- لقد وطدنا العزم علي سعينا لضمان استفادة الجميع من الفرص التي تتيحها تكنولوجيا المعلومات والاتصالات. ونوافق علي أنه ينبغي لمواجهة هذه التحديات أن يعمل جميع أصحاب المصلحة معا لتحسين سبل النفاذ إلي البنية التحتية للمعلومات والاتصالات وإلي تكنولوجيا المعلومات والاتصالات وإلي المعلومات والمعارف، ولبناء القدرات ولزيادة الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، ولإنشاء بيئة تمكينية علي جميع المستويات؛ ولتطوير وتوسيع تطبيقات تكنولوجيا المعلومات والاتصالات، ولتشجيع التنوع الثقافي واحترامه؛ وللاعتراف بنور وسائط الإعلام؛ ولمعالجة الأبعاد الأخلاقية

لمجتمع المعلومات؛ ولتشجيع التعاون الدولي والإقليمي ونوافق علي أن هذه هي المبادئ الرئيسية لبناء مجتمع معلومات جامع.

(١) دور الحكومات وجميع أصحاب المصلحة في النهوض بتكنولوجيا المعلومات والاتصالات من أجل التنمية:

٢٠- تضطلع الحكومات، وكذلك القطاع الخاص والمجتمع المدني والأمم المتحدة والمنظمات الدولية الأخرى، بدور هام وبمسؤولية كبيرة في تطوير مجتمع المعلومات، وكذلك في عمليات صنع القرارات حسب الاقتضاء. وبناء مجتمع معلومات غايته الناس هو جهد مشترك يتطلب التعاون والشراكة بين جميع أصحاب المصلحة.

(٢) البنية التحتية للمعلومات والاتصالات: أساس جوهري لمجتمع معلومات جامع:

٢١- أن التوصيلية عامل تمكيني محوري في بناء مجتمع المعلومات. ويشكل النفاذ الشامل، في كل مكان وعلى أساس منصف وبتكلفة معقولة، إلى البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها بما في ذلك النفاذ إلى الطاقة المحركة وإلى الخدمات البريدية، واحدا من التحديات في مجتمع المعلومات ويجب أن يكون هدفا لجميع أصحاب المصلحة المشتركين في بناء هذا المجتمع. وتنطوي التوصيلية أيضا على النفاذ إلى الطاقة المحركة والخدمات البريدية، وهو ما ينبغي كفالته وفقا للتشريعات المحلية في كل بلد.

٢٢- إن توفر بنية تحتية متطورة من شبكات المعلومات والاتصالات وتطبيقاتها، تكون مكيفة لمراعاة الظروف الإقليمية والوطنية والمحلية ويسهل النفاذ إليها بتكلفة معقولة، وتستغل على نطاق أوسع إمكانات النطاق العريض وغيره من التكنولوجيات المبتكرة حيثما أمكن، من شأنه أن يزيد سرعة التقدم الاجتماعي والاقتصادي في البلدان وأن يعزز رفاه جميع الأفراد والمجتمعات والشعوب.

٢٣- وينبغي وضع سياسات توفر مناخا مؤاتيا من الاستقرار وإمكانية التنبؤ والمنافسة الشريفة علي جميع المستويات وتنفيذ هذه السياسات بحيث لا تؤدي إلي اجتذاب المزيد من الاستثمارات الخاصة من أجل تنمية البنية التحتية لتكنولوجيا المعلومات والاتصالات فحسب وغنما تسمح أيضا بالوفاء بالتزامات الخدمة الشاملة في المناطق التي لا تنجح فيها ظروف السوق التقليدية. ومن شأن إنشاء نقاط لنفاذ الجمهور في المناطق المحرومة إلي تكنولوجيا المعلومات والاتصالات، في أماكن مثل مكاتب البريد والمدارس والمكتبات ودور المحفوظات، أن يكون وسيلة فعالة لضمان النفاذ الشامل إلي البنية التحتية والخدمات التي يوفرها مجتمع المعلومات.

### (٣) النفاذ إلي المعلومات والمعرفة:

٢٤- إن قدرة الجميع علي النفاذ إلي المعلومات والأفكار والمعارف والمساهمة فيها مسألة أساسية في مجتمع معلومات جامع.

٢٥- ومن الممكن تعزيز وتبادل المعارف علي الصعيد العالمي لأغراض التنمية وتدعيمها بإزالة الحواجز التي تعترض سبيل النفاذ المنصف إلي المعلومات لأغراض الأنشطة الاقتصادية والاجتماعية والسياسية والصحية والثقافية والتعليمية والعلمية وتيسير النفاذ إلي المعلومات المشاع، بما في ذلك من خلال التصميمات العالمية واستخدام التكنولوجيات المساعدة.

٢٦- يمثل ثراء ميدان المعلومات المشاع عنصرا ضروريا لنمو مجتمع المعلومات وتحقيق منافع متعددة مثل تنقيف الجمهور، وتوفير فرص العمل الجديدة، والابتكار وتوفير فرص التجارة وتقدم العلوم. وينبغي تيسير النفاذ إلي المعلومات المشاع لدعم مجتمع المعلومات كما ينبغي حمايتها من سوء استغلالها. وينبغي تدعيم المؤسسات العامة مثل المكتبات ودور المحفوظات والمتاحف ومعارض مجموعات الأعمال الثقافية وغيرها من نقاط النفاذ في

المجتمعات المحلية، وذلك لدعم الحفاظ علي السجلات الوثائقية والنفاز الحر والمتصف إلي المعلومات.

٢٧- ويمكن تعزيز النفاز إلي المعلومات والمعارف من خلال إنكاء الوعي بين جميع أصحاب المصلحة بالإمكانات التي توفرها مختلف نماذج البرمجيات، بما فيها البرمجيات مسجلة الملكية والمفتوحة المصدرة والمجانية وذلك لزيادة المنافسة ونفاذ المستعملين وتنوع الاختيار ولتمكين جميع المستخدمين من وضع الحلول التي تفي بمتطلباتهم.والنفاز إلي البرمجيات بتكلفة معقولة ينبغي أن يعتبر عنصرا هاما في مجتمع للمعلومات جامع حقا.

٢٨- ونسعي إلي تعزيز النفاز الشامل إلي المعارف العلمية علي أساس تكافؤ الفرص أمام الجميع واستحداث المعلومات العلمية والتقنية ونشرها، بما في ذلك مبادرات النفاز المفتوح من أجل النشر العلمي.

#### (٤) بناء القدرات:

٢٩- ينبغي أن يتاح لكل شخص فرصة لكتساب المهارات والمعارف اللازمة لفهم مجتمع واقتصاد المعارف والمشاركة فيهما بنشاط والاستفادة الكاملة منها. ومحو الأمية وتوفير التعليم الابتدائي للجميع من العوامل الرئيسية لبناء مجتمع معلومات جامع يولي اهتماما خاصا للاحتياجات التي تنفرد بها الفتيات والنساء. ونظرا لاتساع نطاق تكنولوجيا المعلومات والاتصالات والحاجة علي أخصائيين في المعلومات علي جميع المستويات، فإن عملية بناء القدرات المؤسسية جديرة بعناية خاصة.

٣٠- وينبغي تعزيز استعمال تكنولوجيا المعلومات والاتصالات في جميع مراحل التعليم والتدريب وتنمية الموارد البشرية مع مراعاة الاحتياجات الخاصة للأشخاص المعوقين والمجموعات المحرومة والضعيفة.

٣١- إن مواصلة التعليم وتعليم البالغين وإعادة التدريب، والتعلم مدى الحياة، والتعلم عن بعد، وغير ذلك من الخدمات الخاصة، كالطب عن بعد، يمكنها أن تسهم جوهرياً في زيادة قابلية التوظيف وأن تساعد الناس على الاستفادة من الفرص الجديدة التي تتيحها تكنولوجيا المعلومات والاتصالات للوظائف التقليدية والعمل الحر والمهن الجديدة. وتعتبر التوعية بتكنولوجيا المعلومات والاتصالات ومعرفة مبادئها من بين الركائز الأساسية في هذا المجال.

٣٢- ويتعين على مؤلفي المحتوى وناشريه ومنتجيهم وكذلك على المدرسين والمدرسين وأمناء المحفوظات وأمناء المكتبات والدارسين القيام بدور نشط في تعزيز مجتمع المعلومات، ولا سيما في أقل البلدان نمواً.

٣٣- ولتحقيق التنمية المستدامة لمجتمع المعلومات لابد من تدعيم القدرة الوطنية في البحوث والتطوير في مجال تكنولوجيا المعلومات والاتصالات. وفضلاً عن ذلك، فإن الشراكات، خاصة بين البلدان المتقدمة والبلدان النامية، بما فيها البلدان التي تمر اقتصاداتها بمرحلة تحول، في مجالات البحوث والتطوير، ونقل التكنولوجيا وتصنيع منتجات وخدمات تكنولوجيا المعلومات والاتصالات، وإنتاجها وتسويقها، شراكات ذات أهمية حاسمة في تعزيز بناء القدرات والمشاركة الشاملة في مجتمع المعلومات. ويفتح تصنيع منتجات تكنولوجيا المعلومات والاتصالات آفاقاً واسعة لتكوين الثروات.

٣٤- إن تحقيق طموحنا المشترك، ولا سيما للبلدان النامية، بما فيها البلدان التي تمر اقتصاداتها بمرحلة تحول، للتمتع بالعضوية الكاملة في مجتمع المعلومات، والانتماء الإيجابي في اقتصاد المعرفة، يعتمد إلى حد كبير على زيادة بناء القدرات في مجالات التعليم والدراسة التكنولوجية والنفوذ إلى المعلومات، وهي جميعاً من العوامل الرئيسية في تحديد درجة التنمية والقدرة على المنافسة.

(٥) بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات:

٣٥- إن تعزيز إطار الطمأنينة الذي يشمل أمن المعلومات وأمن الشبكات والتصديق وصون الخصوصية وحماية المستهلك، شرط أساسي مسبق لتنمية مجتمع المعلومات وبناء الثقة بين مستخدمي تكنولوجيا المعلومات والاتصالات. ويتطلب الأمر ترويج ثقافة عالمية للأمن السيبراني وتطويرها وتنفيذها بالتعاون مع جميع أصحاب المصلحة وهيئات الخبرة الدولية. وينبغي دعم هذه الجهود بمزيد من التعاون الدولي. ومن المهم، في إطار هذه الثقافة العالمية للأمن السيبراني، تعزيز الأمن وضمان حماية البيانات والخصوصية مع تعزيز النفاذ والتجارة في الوقت نفسه، وبالإضافة إلى ذلك، يجب أن يؤخذ في الاعتبار مستوى التنمية الاجتماعية والاقتصادية في كل بلد وأن تحترم جوانب مجتمع المعلومات ذات التوجه الإنمائي.

٣٦- وإذ نعترف بمبادئ النفاذ الشامل وغير التمييزي لجميع الأمم غلي تكنولوجيا المعلومات والاتصالات، فإننا ندعم أنشطة الأمم المتحدة التي تحول دون إمكانية استعمال تكنولوجيا المعلومات والاتصالات في أغراض لا تتسق مع الأهداف المتعلقة بصون الاستقرار والأمن الدوليين، وقد تنال من سلامة البنية التحتية داخل الدول، بما يلحق الضرر بأمنها. ومع احترام حقوق الإنسان، فمن الضروري منع استعمال موارد المعلومات والتكنولوجيات في أغراض إجرامية وإرهابية.

٣٧- الرسائل الاحتمالية مشكلة هامة ومتزايدة للمستخدمين والشبكات وللاترنت برمتها. وينبغي تناول مسألة الرسائل الاحتمالية والأمن السيبراني علي المستويات الوطنية والدولية الملانمة.



#### (٦) البيئة التمكينية:

٣٨- لابد لمجتمع المعلومات من بيئة تمكينية علي الصعيد الوطني والدولي. وينبغي استعمال تكنولوجيا المعلومات والاتصالات كأداة هامة رئيسية في الحكم الرشيد.

٣٩- إن سيادة القانون، واقتراثها بوجود سياسة داعمة شفافة تشجع المنافسة وتكون محايدة تكنولوجيا ويمكن التنبؤ بها، وبوجود إطار تنظيمي يعبر عن الواقع الوطني أمر جوهري لبناء مجتمع معلومات غايته الناس. ويتعين علي الحكومات التدخل عند الاقتضاء لتدارك مواطن القصور في السوق، وللحفاظ علي المنافسة النزيهة واجتذاب الاستثمار وتعزيز تنمية البنية التحتية لتكنولوجيا المعلومات والاتصالات وتطبيقاتها ولتعظيم المنافع الاقتصادية والاجتماعية، ولخدمة الأولويات الوطنية.

٤٠- إن توفر بيئة دولية دينامية وتمكينية تدعم الاستثمارجنبي المباشر ونقل التكنولوجيا والتعاون الدولي، لا سيما في مجالات التمويل والنيون والتجارة، إضافة إلي مشاركة كاملة وفعالة من جانب البلدان النامية في عملية صنع القرار عالميا، كل هذه الأمور عناصر حيوية تستكمل جهود التنمية الوطنية المتصلة بتكنولوجيا المعلومات والاتصالات. ومن شأن تحسين التوصيلية العالمية بتكلفة معقولة أن يسهم مساهمة كبيرة في فعالية هذه الجهود الإنمائية.

٤١- إن تكنولوجيا المعلومات والاتصالات عامل هام يمكن من تحقيق النمو من خلال ما توفره من مكاسب في الكفاءة وزيادة في الإنتاجية، لا سيما في المنشآت الصغيرة والمتوسطة. وفي هذا الصدد تتطوي تنمية مجتمع المعلومات علي أهمية للنمو الاقتصادي المرتكز علي قاعدة عريضة سواء في البلدان المتقدمة أو النامية. وينبغي تعزيز المكاسب التي تتحقق علي صعيد

الإنتاجية مؤيدة تكنولوجيا المعلومات والاتصالات بتكنولوجيا المعلومات والاتصالات والابتكارات المطبقة علي مختلف القطاعات الاقتصادية. والتوزيع المنصف للمزايا يسهم في استئصال الفقر وفي التنمية الاجتماعية. والسياسات الرامية إلى تعزيز الاستثمار المنتج وتمكن المنشآت، وخاصة المشاريع الصغيرة والمتوسطة، من أن تدخل التغييرات اللازمة لكي تجني ثمار تكنولوجيا المعلومات والاتصالات، ستكون علي الأرجح أكثر السياسات نفعا.

٤٢- حماية الملكية الفكرية عنصر هام من أجل تشجيع الابتكار والإبداع في مجتمع المعلومات؛ وبالمثل، فإن نشر المعرفة وبثها وتقاسمها علي نطاق واسع عنصر هام لتشجيع الابتكار والإبداع. وتيسير المشاركة المجدية من جانب الجميع في قضايا الملكية الفكرية وتقاسم المعارف، من خلال التوعية وبناء القدرات، جانب أساسي في مجتمع المعلومات الجامع.

٤٣- أفضل طريقة لدفع التنمية المستدامة في مجتمع المعلومات هي الإنماج الكامل للجهود والبرامج المتصلة بتكنولوجيا المعلومات والاتصالات في الاستراتيجيات الإنمائية الوطنية والإقليمية. ونحن نرحب بالشراكة الجديدة من أجل تنمية إفريقيا، وتشجيع المجتمع الدولي علي مساندة التدابير ذات الصلة بتكنولوجيا المعلومات والاتصالات لهذه المبادرة وكذلك التدابير المرتبطة بجهود مماثلة في مناطق أخرى. ويسهم توزيع ثمار النمو المترتبة علي تكنولوجيا المعلومات والاتصالات في استئصال الفقر وفي تحقيق التنمية المستدامة.

٤٤- وتوحيد المقاييس هو إحدى اللبنات الأساسية في بناء مجتمع المعلومات. وينبغي التركيز بشكل خاص علي وضع واعتماد مقاييس دولية. كما أن وضع مقاييس مفتوحة وقابلة للتشغيل البيني وغير تمييزية وتدفعها قوى الطلب، وتأخذ في الاعتبار احتياجات المستعملين والمستهلكين، هو عنصر أساسي في تطوير تكنولوجيا المعلومات والاتصالات وزيادة انتشارها وتيسير النفاذ إليها بتكلفة معقولة، خاصة في البلدان النامية. وترمي المقاييس

الدولية إلى توفير بيئة يستطيع فيها المستهلكون النفاذ إلى الخدمات في شتى أنحاء العالم بغض النظر عن التكنولوجيا التي تدعمها.

٤٥- ينبغي إدارة طيف الترددات الراديوية بما يحقق الصالح العام ويتفق مع مبدأ الشرعية، ومع الاحترام الكامل للقوانين والتشريعات الوطنية والاتفاقات الدولية ذات الصلة.

٤٦- وتستحدث الدول بقوة، في غضون بناء مجتمع المعلومات، علي اتخاذ خطوات لمنع وتحاشي أية تدابير من جانب واحد لا تتفق مع القانون الدولي وميثاق الأمم المتحدة ويمكن أن تعرقل التحقيق الكامل للتنمية الاقتصادية والاجتماعية للسكان في البلدان المعنية أو تعوق رفاههم.

٤٧- واعترافاً بأن تكنولوجيا المعلومات والاتصالات تغير طريقة عملنا تغييراً مضطرباً، فمن الأمور الأساسية توفير بيئة عمل آمنة ومأمونة وصحية وملائمة لاستخدام تكنولوجيا المعلومات والاتصالات، وتحترم المعايير الدولية ذات الصلة.

٤٨- وقد تطورت الإنترنت لتصبح مرفقاً عالمياً متاحة للعامّة وينبغي أن تشكل إدارتها قضية مركزية في جدول أعمال مجتمع المعلومات. وينبغي أن تكون الإدارة الدولية للإنترنت متعددة الأطراف وشفافة وديموقراطية، وبمشاركة كاملة من الحكومات والقطاع الخاص والمجتمع المدني والمنظمات الدولية. ويجب أن تكفل توزيعاً منصفاً للموارد وأن تيسر النفاذ أمام الجميع وأن تكفل تشغيلاً مستقراً وأماناً للإنترنت مع مراعاة اعتبار تعدد اللغات.

٤٩- تتطوي إدارة الإنترنت علي قضايا تقنية وقضايا تتعلق بالسياسات العامة علي حد سواء، وينبغي أن يشترك فيها جميع أصحاب المصلحة والمنظمات الدولية الحكومية والمنظمات الدولية ذات الصلة. ومن المسلم به في هذا الصدد أن:

أ) السلطة السياسية علي قضايا السياسات العامة المتصلة بالإنترنت تعتبر حقاً سيادياً للدول، إذ تملك حقوقاً ومسؤوليات بشأن قضايا السياسات العامة الدولية المتصلة بالإنترنت.

ب) ظل القطاع الخاص يؤدي دوراً هاماً في تطوير الإنترنت في المجالين التقني والاقتصادي، وينبغي له أن يواصل القيام بذلك؛

ج) كما قام المجتمع المدني بدور هام في المسائل المتعلقة بالإنترنت وبخاصة علي صعيد المجتمع المحلي وينبغي له أن يواصل القيام بهذا الدور؛

د) قامت المنظمات الدولية الحكومية بدور في تيسير تنسيق قضايا السياسات العامة المتصلة بالإنترنت وينبغي أن تواصل القيام بذلك؛

هـ) كما قامت المنظمات الدولية بدور هام في تطوير المعايير التقنية المتصلة بالإنترنت والسياسات ذات الصلة، وينبغي أن تواصل القيام بذلك.

٥٠- ينبغي معالجة القضايا المتعلقة بإدارة الإنترنت علي الصعيد الدولي بطريقة منسقة. إننا نطلب من الأمين العام للأمم المتحدة أن ينشئ فريق عمل معني بإدارة الإنترنت في عملية مفتوحة وجامعة تكفل إيجاد آلية للمشاركة الكاملة والنشطة في جانب الحكومات والقطاع الخاص والمجتمع المدني من البلدان المتقدمة والنامية علي حد سواء، وتشمل المنظمات والمحافل الدولية الحكومية والدولية، وبحيث يستكشف ويقدم اقتراحات، بحسب الاقتضاء، بشأن اتخاذ إجراءات تتعلق بإدارة الإنترنت بحلول عام ٢٠٠٥.

(٧) تطبيقات تكنولوجيا المعلومات والاتصالات ومنافعها في جميع جوانب الحياة:

٥١- ينبغي أن يكون الهدف من استعمال تكنولوجيا المعلومات والاتصالات ونشرها هو تحقيق فوائد في كل جوانب حياتنا اليومية وتطبيقات تكنولوجيا المعلومات والاتصالات تتطوي علي أهمية في العمليات والخدمات

الحكومية والرعاية الصحية والمعلومات الصحية والتعليم والتدريب والعمل وتوفير فرص العمل والأعمال التجارية والزراعة والنقل وحماية البيئة وإدارة الموارد الطبيعية ومنع الكوارث والثقافة واستئصال الفقر وغيرها من الأهداف الإنمائية المتفق عليها. كذلك ينبغي أن تسهم تكنولوجيا المعلومات والاتصالات في إشاعة أنماط مستدامة للإنتاج والاستهلاك وفي خفض الحواجز التقليدية، وبالتالي إتاحة الفرصة أمام الجميع للنفوذ إلى الأسواق المحلية والعالمية بطريقة تتسم بمزيد من الإنصاف. وينبغي أن تكون كافية للاحتياجات المحلية من حيث اللغة والثقافة، وأن تدعم التنمية المستدامة، ولهذا الغرض، ينبغي أن تؤدي السلطات المحلية دورا رئيسيا في توفير خدمات تكنولوجيا المعلومات والاتصالات لصالح مواطنيها.

#### (٨) التنوع الثقافي والهوية الثقافية، والتنوع اللغوي والمحتوي المحلي:

٥٢- التنوع الثقافي هو التراث المشترك للإنسانية جمعاء. وينبغي أن يقوم مجتمع المعلومات على أساس احترام الهوية الثقافية والتنوع الثقافي واللغوي والتقاليد والأديان وأن يعزز احترام هذه المفاهيم، وأن يشجع الحوار بين الثقافات والحضارات. ومن شأن تعزيز وتأكيد الهويات الثقافية المتنوعة واللغات المختلفة والحفاظ عليها، كما جاء في الوثائق المتفق عليها ذات الصلة الصادرة عن الأمم المتحدة، بما في ذلك إعلان اليونسكو العالمي بشأن التنوع الثقافي، أن يدعم إثراء مجتمع المعلومات.

٥٣- ويجب إعطاء أولوية عالية في بناء مجتمع معلومات جامع لإنشاء المحتوى بلغات وأنساق متعددة ونشره والحفاظ عليه مع إيلاء الاهتمام اللازم إلى تنوع مصادر العمال الإبداعية والاعتراف الواجب بحقوق المؤلفين والفنانين، ومن الضروري تعزيز إنتاج شتى أنواع المحتوى- التربوية أو العلمية أو الثقافية أو الترفيهية- بلغات وأنساق متنوعة والنفوذ إليها. كما أن تطوير محتوى محلي يناسب الاحتياجات المحلية أو الإقليمية يشجع التنمية

الاجتماعية والاقتصادية ويحفز مشاركة جميع أصحاب المصلحة، بمن فيهم الناس الذين يعيشون في المناطق الريفية والنائية والهامشية.

٥٤- إن الحفاظ علي التراث الثقافي هو عنصر حاسم في تكوين الهوية وفهم الأفراد لذاتهم وربط المجتمع بماضيه. وينبغي لمجتمع المعلومات أن يعمل علي تسخير التراث الثقافي والحفاظ عليه للمستقبل بكل الوسائل المناسبة، بما فيها الرقمنة.

#### (٩) وسائط الإعلام:

٥٥- ونؤكد من جديد التزامنا بمبادئ حرية الصحافة وحرية المعلومات وكذلك بمبادئ الاستقلال والتعددية والتنوع في وسائط الإعلام، وهي عناصر جوهرية في مجتمع المعلومات، ومن الأمور الهامة في مجتمع المعلومات حرية التماس المعلومات وتلقيها وإذاعتها واستعمالها لإحداث وتراكم ونشر المعرفة. ندعو وسائط الإعلام إلي استعمال المعلومات بطريقة تتم عن الشعور بالمسؤولية وفقا لأعلي المعايير الأخلاقية والمهنية. وتؤدي وسائط الإعلام التقليدية بجميع أشكالها دورا هاما في مجتمع المعلومات، وينبغي أن تؤدي تكنولوجيا المعلومات والاتصالات دورا داعما في هذا الصدد. وينبغي تشجيع تنوع ملكية وسائط الإعلام بما يتفق مع القوانين الوطنية مع مراعاة الاتفاقيات الدولية ذات الصلة. ونؤكد من جديد ضرورة الحد من اختلال التوازن في وسائط الإعلام علي الصعيد الدولي ولا سيما فيما يتعلق بالبنية التحتية والموارد التقنية وتنمية المهارات البشرية.

#### (١٠) الأبعاد الأخلاقية لمجتمع المعلومات:

٥٦- ينبغي لمجتمع المعلومات أن يحترم السلم وأن يدافع عن القيم الأساسية مثل الحرية والمساواة والتضامن والتسامح والمسؤولية المشتركة واحترام الطبيعة.

٥٧- وإننا نقر بأهمية الأخلاق لمجتمع المعلومات، الذي ينبغي أن يراعى العدالة وكرامة الإنسان وقيمه. وينبغي توفير أقصى حد ممكن من الحماية للأسرة لتمكينها من أداء دورها الحاسم في المجتمع.

٥٨- ينبغي أن يراعى في استعمال تكنولوجيا المعلومات والاتصالات وخلق المحتوى احترام حقوق الإنسان والحريات الأساسية للآخرين، بما في ذلك الخصوصية الشخصية والحق في حرية الفكر والضمير والدين تمشيا مع الصكوك الدولية ذات الصلة.

٥٩- ينبغي لجميع الأطراف الفاعلة في مجتمع المعلومات أن تتخذ الإجراءات المناسبة والتدابير الوقائية، حسبما تقرره القوانين، لمناهضة استخدام تكنولوجيا المعلومات والاتصالات في أعراض سيئة مثل العمال غير المشروعة وغير ذلك من الأعمال بدوافع العنصرية والتمييز العنصري وكرهية الأجانب وما يتصل بها من أشكال التعصب والكرهية والعنف، وجميع أشكال الاعتداء على الأطفال، بما فيها اشتهااء الأطفال، واستغلال الأطفال في المواد الإباحية، والاتجار بالأشخاص واستغلالهم.

#### (١١) التعاون الدولي والإقليمي:

٦٠- إننا نسعى إلى الاستفادة الكاملة من الفرص التي تتيحها تكنولوجيا المعلومات والاتصالات في جهودنا لبلوغ الأهداف الإنمائية المتفق عليها دولياً، بما فيها الأهداف الواردة في إعلان الألفية، ولدعم المبادئ الرئيسية الواردة في هذا الإعلان. إن مجتمع المعلومات عالمي الطابع في جوهره، ومن ثم لا بد من تدعيم الجهود الوطنية، بإقامة تعاون دولي وإقليمي فعال بين الحكومات والقطاع الخاص والمجتمع المدني وأصحاب المصلحة الآخرين، بما في ذلك المؤسسات المالية الدولية.

٦١- ولكي يتسنى بناء مجتمع معلومات عالمي جامع، سوف نعتمد علي التماس مناهج وآليات دولية ملموسة وفعالية العمل بموجبها، بما في ذلك المساعدة المالية والتقنية، ولذا، ومع تقديرنا لما يجري من تعاون بشأن تكنولوجيا المعلومات والاتصالات من خلال آليات مختلفة، فإننا ندعو جميع أصحاب المصلحة إلي الالتزام "بجدول أعمال التضامن الرقمي" الوارد في خطة العمل. ونحن مقتنعون أن الهدف المتفق عليه عالميا هو المساهمة في سد الفجوة الرقمية، وتعزيز النفاذ إلي تكنولوجيا المعلومات والاتصالات، وإيجاد فرص رقمية وتسخير إمكانات تكنولوجيا المعلومات والاتصالات لصالح التنمية. ونقر الرغبة التي أبدتها بعض المشاركين في إنشاء صندوق طوعي دولي "هو صندوق التضامن الرقمي"، ورغبة بعض المشاركين الآخرين في إجراء دراسات عن الآليات القائمة وعن جنوى هذا الصندوق ومدى كفاءته.

٦٢- إن التكامل الإقليمي يسهم في تنمية مجتمع المعلومات العالمي ويجعل التعاون الوثيق داخل الأقاليم وفيما بينها أمرا لا غني عنه. وينبغي للحوار الإقليمي أن يسهم في بناء القدرات الوطنية وفي موازنة الاستراتيجيات الوطنية مع أهداف إعلان المبادئ هذا موازنة متسقة، وأن يراعي في الوقت ذاته الخصائص الوطنية والإقليمية. وفي هذا السياق نرحب بالتدابير المتصلة بتكنولوجيا المعلومات والاتصالات في إطار هذه المبادرات وتشجع المجتمع الدولي علي دعم هذه التدابير.

٦٣- ونقرر مساعدة البلدان النامية واقل البلدان نموا والبلدان التي تمر اقتصاداتها بمرحلة تحول، وذلك من خلال تعبئة التمويل من كل المصادر وتوفير المساعدة المالية والتقنية وإيجاد بيئة مؤاتية لنقل التكنولوجيا بما يتسق مع مقاصد هذا الإعلان وخطة العمل.

٦٤- إن الاختصاصات الرئيسية للاتحاد الدولي للاتصالات في مجالات تكنولوجيا المعلومات والاتصالات والمساعدة علي سد الفجوة الرقمية



والتعاون الدولي والإقليمي، وإدارة طيف التردد الراديوي، ووضع المعايير ونشر المعلومات، كلها عوامل ذات أهمية حاسمة في بناء مجتمع المعلومات.

#### نحو مجتمع معلومات للجميع يركز علي تقاسم المعرفة:

٦٥- إننا نلتزم بتعزيز التعاون من أجل البحث عن استجابات مشتركة للتحديات التي نواجهها ومن أجل تنفيذ خطة العمل التي ستحقق رؤيتنا لمجتمع معلومات جامع يركز علي المبادئ الرئيسية الواردة في هذا الإعلان.

٦٦- ونلتزم كذلك بتقييم ومتابعة التقدم المحرز في سد الفجوة الرقمية، مع مراعاة مستويات التنمية المختلفة، وذلك لتحقيق الأهداف الإنمائية المنققة عليها دولياً، بما في ذلك الأهداف المبينة في إعلان الألفية، ولتقييم فعالية الاستثمار وجهود التعاون الدولي في بناء مجتمع المعلومات.

٦٧- ويحدونا الاعتقاد الراسخ بأننا مجتمعين ندخل عهداً جديداً ينطوي علي إمكانات هائلة، هو عهد مجتمع المعلومات واتساع أفق الاتصال بين الناس. وفي هذا المجتمع الناشئ يمكن إنشاء المعلومات والمعارف وتبادلها وتقاسمها وبثها عبر جميع شبكات العالم. وإذا اتخذنا التدابير اللازمة فيستطيع الجميع في القريب العمل معا لبناء مجتمع معلومات جديد يقوم علي تقاسم المعرفة ويرتكز علي التضامن العالمي وعلي تبادل فهم أفضل بين الشعوب والأمم. ونحن علي ثقة من أن هذه التدابير تمهد الطريق لتنمية مجتمع معرفة حقيقي في المستقبل.

## مذكرة من الأمانة التنفيذية

### مشروع جدول الأعمال

#### لمرحلة تونس من القمة العالمية لاجتماع المعلومات

- ١- افتتاح مرحلة تونس من القمة العالمية لمجتمع المعلومات.
- ٢- انتخاب رئيس القمة العالمية ورئيس الاجتماع التنظيمي.
- ٣- إقرار جدول الأعمال.
- ٤- تعديل المادة ٧ من النظام الداخلي للقمة.
- ٥- انتخاب أعضاء مكتب القمة الآخرين.
- ٦- تنظيم الأعمال.
- ٧- أوراق اعتماد الممثلين في القمة:  
(أ) تعيين أعضاء لجنة أوراق الاعتماد.  
(ب) تقرير لجنة أوراق الاعتماد.
- ٨- تقرير اللجنة التحضيرية.
- ٩- المناقشة العامة.
- ١٠- الموائل المستديرة والأفرقة رفيعة المستوى.
- ١١- تقرير من اجتماعات أصحاب المصلحة المتعددين.
- ١٢- اعتماد الوثيقة (الوثائق) الختامية<sup>(١)</sup>.
- ١٣- اعتماد تقرير مرحلة تونس من القمة العالمية.
- ١٤- اختتام القمة.

---

(١) ستستخدم إما كلمة "الوثيقة" أو "الوثائق" (بالمفرد أو الجمع) حسب عدد الوثائق.

## مذكرة من الأمانة التنفيذية

### مشروع النسق المقترح لمرحلة تونس

#### لل قمة العالمية لمجتمع المعلومات

١- ستعقد مرحلة تونس للقمة العالمية لمجتمع المعلومات في أرض المعارض في كرم بتونس العاصمة في الفترة من الأربعاء ١٦ نوفمبر إلى الجمعة ١٨ نوفمبر ٢٠٠٥. وستألف القمة من اجتماع تنظيمي وحفل افتتاح وثمانتي جلسات عامة، واجتماعات الموائد المستديرة وأفرقة المناقشة رفيعة المستوى. ويتضمن الملحق ١ وصفا لخطة تنظيم الوقت في القمة.

٢- ستبدأ مرحلة تونس للقمة العالمية بالاجتماع التنظيمي الذي يعقد صباح يوم الأربعاء ويفتتحه الأمين العام للأمم المتحدة أو أي شخص يختاره له لهذا الغرض. وسيقوم الاجتماع بانتخاب رئيس القمة ورئيس الاجتماع التنظيمي. وسيستمر الاجتماع بعد ذلك تحت رئاسة رئيس الاجتماع التنظيمي، ثم يقوم باعتماد جدول أعمال القمة وتعديل المادة ٧ من نظامها الداخلي وانتخاب أعضاء المكتب والإحاطة علما بتنظيم العمل وتشكيل لجنة أوراق الاعتماد والاستماع إلى تقرير اللجنة التحضيرية.

٣- وبعد الاجتماع التنظيمي، ستعقد مراسم افتتاحية للقمة وسيدعي رئيسا دولتي البلدين المضيفين والأمين العام للأمم المتحدة والأمين العام للاتحاد الدولي للاتصالات ورئيس اللجنة التحضيرية وممثل رفيع المستوى من أحد كيانات المجتمع المدني (بما فيها المنظمات غير الحكومية) علاوة على ممثلي رفيع المستوى من أحد كيانات قطاع الأعمال (بما فيها أعضاء قطاعات الاتحاد الدولي للاتصالات) يتم تعيينهما من خلال آليات التنظيم الذاتي لهذه الكيانات وبالتنسيق مع الأمين العام للقمة، للإدلاء ببيانات افتتاحية.

٤- وبعد حفل الافتتاح مباشرة، ستبدأ الجلسة العامة الأولى بمناقشة عامة وسوف تستمر المناقشة العامة حتى الجلسة العامة الثامنة بعد ظهر يوم الجمعة. وستخصص آخر ١٥ دقيقة من المناقشة العامة في الجلسة العامة الأولى ونصف الساعة الأخيرة في الجلسات الثانية والثالثة والخامسة والسادسة والساعة الأخيرة في الجلستين العامتين الرابعة والسابعة لبيانات ممثلي المنظمات والكيانات الحاضرة في القمة بصفة مراقب.

٥- وسوف توضع قائمة الدول المتحدثة في المناقشة العامة بإجراء قرعة وفقاً للبروتوكول المعتاد في الأمم المتحدة الذي يكفل أن يتحدث رؤساء الدول أو الحكومات أولاً، يليهم الوزراء ورؤساء الوفود الآخرون. وستحدد مدة إلقاء البيان بخمس دقائق. ويسمح لوفد كل حكومة بإلقاء بيان واحد فقط. وستشارك فلسطين أيضاً، بوصفها مراقباً، في المناقشة العامة.

٦- وفي الوقت المخصص للمراقبين، ستحدد مدة إلقاء البيانات بثلاث دقائق. وينبغي أن يمثل جميع المتحدثين أعلى مستوى لمنظماتهم أو كياناتهم. وفيما يتعلق بالكيانات المعتمدة من المجتمع المدني (بما فيها المنظمات غير الحكومية) وقطاع الأعمال (بما فيها أعضاء قطاعات الاتحاد الدولي للاتصالات)، سيتم تحديد المتحدثين باسمها بواسطة آلياتها التنظيمية الخاصة، بالتنسيق مع الأمين العام للقمة. وفيما يتعلق بالمنظمات الدولية الحكومية، يمكن، من ناحية المبدأ، لأعضاء اللجنة رفيعة المستوى لتنظيم القمة، الممثلين علي أعلى مستوى ممكن، الإدلاء ببيانات.

٧- وفي آخر ١٥ دقيقة من الجلسة العامة الخامسة وقرابة الساعة الأخيرة من الجلسة العامة الثامنة وبعد استكمال المناقشة العامة ستستمتع القمة إلى تقارير من اجتماعات مختلف أصحاب المصلحة التي عقدت بالتوازي مع القمة. وسيقوم الأمين العام للقمة بالتنسيق مع اللجنة رفيعة المستوى لتنظيم القمة وآليات التنظيم الذاتي لكيانات المجتمع المدني (بما فيها

المنظمات غير الحكومية) وكيانات قطاع الأعمال بما فيها أعضاء قطاعات الاتحاد) وذلك لتحديد قائمة الاجتماعات التي تقدم تقاريرها إلى الجلسة العامة. وستعطي الأولوية للاجتماعات التي توفر مدخلات إيجابية لأهداف القمة الموضحة في إعلان المبادئ وخطة العمل وكذلك في الوثيقة (الوثائق) الختامية التي ستعتمدها مرحلة تونس من القمة أو ستعطي هذه الأولوية للاجتماعات المتصلة بإنشاء مشاريع شراكة مستدامة لمختلف أصحاب المصلحة.

٨- وفي وقت متأخر من بعد ظهر يوم الجمعة، وبعد الاستماع إلى تقرير لجنة أوراق الاعتماد ستعتمد الجلسة العامة الأخيرة الوثيقة (الوثائق) الختامية وتعتمد تقرير مرحلة تونس من القمة. وبعد ذلك تستمع إلى الكلمات الختامية التي يلقيها رئيسا دولتي البلدين المضيفين والأمين العام للقمة.

٩- وستعقد اجتماعات الموائد المستديرة وأفرقة المناقشة رفيعة المستوى أثناء القمة، بالتوازي مع الجلسات العامة في المقر الرسمي لانعقاد القمة. ويرد صوف اجتماعات الموائد المستديرة وأفرقة المناقشة رفيعة المستوى في الملحقين ٢ و ٣ علي التوالي. وسيحدد الأمين العام للقمة بالتشاور مع مكتب اللجنة التحضيرية والمجموعات الإقليمية، تفاصيل اجتماعات الموائد المستديرة وأفرقة المناقشة رفيعة المستوى.

١٠- وستتاح للمراقبين الدخول مباشرة إلى المقر الرسمي لانعقاد القمة. ونظرا إلى ضيق المكان، سيسمح لعدد محدود من المشاركين من الكيانات المعتمدة من المجتمع المدني (بما فيها المنظمات غير الحكومية) وكيانات قطاع الأعمال (بما فيها أعضاء قطاعات الاتحاد الدولي للاتصالات) بحضور الجلسات العامة، وستقوم الأمانة التنفيذية بإخطار المراقبين بهذه الترتيبات حالما يتم الانتهاء من وضع برنامج القمة.

الملحق ١ خطة تنظيم الوقت لمرحلة تونس من القمة

الجمعة ١٨ نوفمبر		الخميس ١٧ نوفمبر		الأربعاء ١٦ نوفمبر	
من الساعة 0900 إلى الساعة 1300 الجلسة العامة السابعة.	من الساعة 0900 إلى الساعة 1300 الجلسة العامة الرابعة.	من الساعة 0900 إلى الساعة 1300 الجلسة العامة الخامسة (*)	من الساعة 0900 إلى الساعة 1300 الجلسة العامة السادسة (*)	من الساعة 0830 إلى الساعة 0915 الاجتماع التأسيسي	من الساعة 0830 إلى الساعة 0915 الاجتماع التأسيسي
٩. المناقشة العامة (*)	٩. المناقشة العامة (*)	٩. المناقشة العامة (*)	٩. المناقشة العامة (*)	٩. المناقشة العامة (*)	٩. المناقشة العامة (*)
ساعة واحدة المر القبول	ساعة واحدة المر القبول	ساعة واحدة المر القبول	ساعة واحدة المر القبول	١٥ دقيقة المر القبول	١٥ دقيقة المر القبول
من الساعة 1300 إلى الساعة 1400 استراحة	من الساعة 1300 إلى الساعة 1400 استراحة	من الساعة 1300 إلى الساعة 1400 استراحة	من الساعة 1300 إلى الساعة 1400 استراحة	من الساعة 1300 إلى الساعة 1500 استراحة	من الساعة 1300 إلى الساعة 1500 استراحة
من الساعة 1400 إلى الساعة 1900 الجلسة العامة الثامنة	من الساعة 1400 إلى الساعة 1900 الجلسة العامة الثامنة	من الساعة 1400 إلى الساعة 1700 الجلسة العامة الخامسة (*)	من الساعة 1400 إلى الساعة 1700 الجلسة العامة الخامسة (*)	من الساعة 1500 إلى الساعة 1800 الجلسة العامة الثانية	من الساعة 1500 إلى الساعة 1800 الجلسة العامة الثانية
٩. المناقشة العامة (*)	٩. المناقشة العامة (*)	٩. المناقشة العامة (*)	٩. المناقشة العامة (*)	٩. المناقشة العامة (*)	٩. المناقشة العامة (*)
١١ تقرير من اجتماعات مختلف أصحاب المصلحة.	١١ تقرير من اجتماعات مختلف أصحاب المصلحة.	١١ تقرير من اجتماعات مختلف أصحاب المصلحة.	١١ تقرير من اجتماعات مختلف أصحاب المصلحة.	٣٠ دقيقة المر القبول	٣٠ دقيقة المر القبول
٧ (ب) تقرير لجنة أوراق الاعتماد.	٧ (ب) تقرير لجنة أوراق الاعتماد.	٧ (ب) تقرير لجنة أوراق الاعتماد.	٧ (ب) تقرير لجنة أوراق الاعتماد.		
١٢ اعتماد الوثيقة (الوثائق) القتامية	١٢ اعتماد الوثيقة (الوثائق) القتامية	١٢ اعتماد الوثيقة (الوثائق) القتامية	١٢ اعتماد الوثيقة (الوثائق) القتامية		
١٣ اعتماد تقرير مرحلة تونس من القمة.	١٣ اعتماد تقرير مرحلة تونس من القمة.	١٣ اعتماد تقرير مرحلة تونس من القمة.	١٣ اعتماد تقرير مرحلة تونس من القمة.		
١٤ اختتام القمة.	١٤ اختتام القمة.	١٤ اختتام القمة.	١٤ اختتام القمة.		
		٣٠ دقيقة المر القبول.	٣٠ دقيقة المر القبول.		٣٠ دقيقة المر القبول.
					من الساعة 1800 إلى الساعة 2000 الجلسة العامة الثالثة.
					٩. المناقشة العامة (*)

## الملحق ٢ تنظيم اجتماعات الموائد المستديرة(\*)

- ١- سيتم تنظيم اجتماعات الموائد المستديرة لإتاحة الفرصة لرؤساء الدول أو الحكومات للمشاركة في مناقشات تفاعلية بشأن مستقل مجتمع المعلومات مع قيادات المنظمات والكيانات الحاضرة في القمة بصفة مراقب.
- ٢- وسيشترك في كل اجتماع مائدة مستديرة ٢٠ مشاركاً كحد أقصى. وسيكون نصف المشاركين من الدول والنصف الآخر من المنظمات والكيانات الحاضرة في القمة بصفة مراقب.
- ٣- وسيدعو الأمين العام للقمة رؤساء الدول أو الحكومات إلى المشاركة في أحد هذه الاجتماعات. وسيدعي الوزراء إذا استدعي الأمر لكفالة تحقيق التوازن الإقليمي بين المشاركين من الدول. وفي حالة الضرورة سيتم التشاور مع المنسقين الإقليميين للدول للمساعدة على كفالة التوازن الإقليمي في كل اجتماع مائدة مستديرة.
- ٤- وسيحدد الأمين العام للقمة عدد اجتماعات الموائد المستديرة ومواعيدها.
- ٥- وسيكون تنظيم اجتماعات الموائد المستديرة حول موضوع واحد عريض وشامل ومتصل بمختلف الاهتمامات، وسيقوم الأمين العام للقمة بتحديد هذا الموضوع.
- ٦- وسيقوم بإدارة كل اجتماع مائدة مستديرة شخصية بارزة يعينها الأمين العام للقمة.
- ٧- وسيعين الأمين العام للقمة المشاركين من المنظمات والكيانات الحاضرة في القمة بصفة مراقب، وذلك بالتشاور مع اللجنة رفيعة المستوى

(\*) سيحدد الأمين العام للقمة، بالتشاور مع مكتب اللجنة التحضيرية والمجموعات الإقليمية، تفاصيل اجتماعات الموائد المستديرة.

لتنظيم القمة ومع اليات التنظيم الذاتي لكيانات المجتمع المدني (بما فيها غير الحكومية) وكيانات قطاع الأعمال (بما فيها أعضاء قطاعات الاتحاد الدولي للاتصالات).

٨- وستعقد اجتماعات الموائد المستديرة في غرفة يقتصر الدخول إليها على المشاركين ومستشاريهم. وستداع مداولات هذه الاجتماعات فوراً من خلال الإنترنت.

٩- وسيرفق تقرير اجتماعات الموائد المستديرة بالتقرير النهائي للقمة.



### الملحق ٣ تنظيم اجتماعات أفرقة المناقشة رفيعة المستوى<sup>(\*)</sup>

- ١- ستتظم اجتماعات أفرقة المناقشة رفيعة المستوى لكي تتيح للمشاركين في القمة، بما في ذلك المراقبون، منتدى ديناميا للمناقشة والحوار بشأن مستقبل مجتمع المعلومات.
- ٢- سيتألف كل فريق من عدد يصل إلى خمس شخصيات بارزة من نوي الخبرة في موضوع المناقشة.
- ٣- سيعين الأمين العام للقمة أعضاء هذه الأفرقة بالتشاور مع المنسقين الإقليميين للدول واللجنة رفيعة المستوى لتنظيم القمة وآليات التنظيم الذاتي لكيانات المجتمع المدني (بما فيها المنظمات غير الحكومية) وكيانات قطاع الأعمال (بما فيها أعضاء قطاعات الاتحاد الدول للاتصالات).
- ٤- سيعين الأمين العام للقمة عدد أفرقة المناقشة ومواعيدها وموضوعاتها.
- ٥- سيدير مناقشة كل فريق شخصية بارزة يعينها الأمين العام للقمة. وسيحافظ مديرو المناقشات على حيوية المناقشات وتفاعلها مع تشجيع الجمهور على توجيه الأسئلة وإبداء التعليقات.
- ٦- ستعقد الأفرقة في قاعات تتيح للجمهور مشاهدة المناقشات والمشاركة فيها. وستداع مداولات هذه الأفرقة فوراً من خلال الإنترنت.
- ٧- سترفق تقارير الأفرقة بالتقرير النهائي للقمة.

(\*) سيحدد الأمين العام للقمة، بالتشاور مع مكتب اللجنة التحضيرية والمجموعات الإقليمية، تفاصيل اجتماعات أفرقة المناقشة رفيعة المستوى.

## **النظام الداخلي للجنة لاجتماع المعلومات**

**أولاً: التمثيل وأوراق الاعتماد:**

### **المادة ١**

#### **تشكيل الوفود**

يتألف وفد كل دولة مشاركة في القمة ووفد الجماعة الأوروبية، من رئيس للوفد وغيره من الممثلين الذين يتطلبهم تشكيل الوفد.

### **المادة ٢**

#### **المنوبون والمستشارون**

يجوز لرئيس الوفد أن يسمي أي ممثل مناوب أو مستشار للتصرف بصفة ممثل.

### **المادة ٣**

#### **إصدار أوراق الاعتماد**

في كل مرحلة من مرحلتي القمة، تصدر أوراق الاعتماد عن رئيس الدولة أو الحكومة أو عن وزير الشؤون الخارجية أو تصدر في حالة الجماعة الأوروبية عن رئيس المفوضية الأوروبية.

### **المادة ٤**

#### **تقديم أوراق الاعتماد**

تقدم أوراق اعتماد الممثلين وأسماء الممثلين المناوبين والمستشارين إلي الأمين العام للقمة قبل التاريخ المحدد لافتتاح القمة بأسبوع علي الأقل إن أمكن.

## المادة ٥

### لجنة أوراق الاعتماد

يتم في بداية القمة تعيين لجنة لأوراق الاعتماد تتألف من تسعة أعضاء. ويستند تشكيل اللجنة إلي تشكيل لجنة وثائق التفويض للجمعية العامة للأمم المتحدة وقت انعقاد القمة في كل مرحلة من مرحلتها. وتخصص اللجنة أوراق اعتماد الممثلين وتقديم تقريراً إلي القمة دون تأخير.

## المادة ٦

### المشاركة في القمة علي أساس مؤقت

يحق للممثلين المشاركة في القمة علي أساس مؤقت انتظاراً لقرار القمة بشأن أوراق اعتمادهم.  
ثانياً: أعضاء المكتب:

## المادة ٦

### الانتخابات

تنتخب القمة من بين ممثلي الدول المشاركة أعضاء المكتب التاليين: رئيس وثلاثون نائباً للرئيس يقوم أحدهم بعمل المقرر علي أن يكون انتخاب هؤلاء المسؤولين علي أساس كفاءة الطابع التمثيلي للمكتب، كما تنتخب نائبين حكيمين للرئيس يرشحهما البلدان المضيفان للقمة. ويجوز للقمة أيضاً أن تنتخب أي أعضاء آخرين للمكتب حسبما تراه ضرورياً لأداء وظائفها.

## المادة ٨

### السلطات العامة للرئيس

١- بالإضافة إلي ممارسة السلطات الممنوحة للرئيس في مواد أخرى من هذا النظام، يقوم الرئيس برئاسة الجلسات العامة للقمة ويعلن افتتاح كل جلسة

واختتامها ويعرض المسائل لاتخاذ القرار بشأنها ويعرض المسائل للتصويت إذا استلزم الأمر ويعلن القرارات. ويبت الرئيس في النقاط النظامية ويتمتع رهنا بهذا النظام الداخلي، بالسيطرة على سير المداولات والمحافظة على النظام فيها. وللرئيس أن يقترح على القمة قفل قائمة المتحدثين وتحديد الزمن المسموح به للمتحدثين وتحديد عدد المرات التي يجوز فيها لكل ممثل أن يتحدث بشأن أي مسألة وإرجاء أو إنهاء المناقشة وتعليق أو رفع الجلسة أو أي اقتراح آخر إجرائي يراه ملائما.

٢- يظل الرئيس تحت سلطة القمة في ممارسة وظائفه.

#### **المادة ٩**

##### **القائم بأعمال الرئيس**

١- يسمي الرئيس أحد نواب الرئيس ليحل محله إذا تغيب عن جلسة أو جزء من جلسة.

٢- يتمتع نائب الرئيس الذي يقوم بعمل الرئيس بنفس سلطات الرئيس ويتكفل بنفس واجباته.

#### **المادة ١٩**

##### **تبديل الرئيس**

ينتخب رئيس جديد إذا عجز الرئيس عن أداء وظائفه.

ثالثا: المكتب:

#### **المادة ١١**

##### **التشكيل**

يتألف المكتب من الرئيس ونواب الرئيس الذين يقوم أحدهم بعمل المقرر. ويعمل الرئيس أو نائبه الذي يسميه في حالة غيابه رئيسا للمكتب. ويجوز

لرئيس لجنة أوراق الاعتماد أو رئيس كل لجنة أخرى تنشئها القمة وفقا للمادة ٤٤ المشاركة في المكتب دون أن يكون لهم الحق في التصويت.

#### **المادة ١٢**

##### **الوظائف**

يساعد المكتب الرئيس في تسيير أعمال القمة عموما ويكفل، رهنا بقرارات القمة، تنسيق أعمالها.  
رابعاً: أمانة القمة:

#### **المادة ١٣**

##### **واجبات الأمين العام للقمة**

- ١- يعمل الأمين العام للاتحاد الدولي للاتصالات أو من يسميه ممثلاً عنه بصفة الأمين العام للقمة في جميع جلسات القمة وهيئاتها الفرعية ويقوم بإدارة موظفي الأمانة.
- ٢- يجوز للأمين العام للقمة أن يسمي عضواً من أمانة القمة ليحل محله في هذه الاجتماعات.

#### **المادة ١٤**

##### **واجبات أمانة القمة**

- تقوم أمانة القمة بما يلي، تحت إشراف القمة ووفقاً لهذا النظام الداخلي:
- (أ) توفير الترجمة الشفوية للجلسات.
  - (ب) استلام وثائق القمة وترجمتها وتعميمها.
  - (ج) نشر وتعميم الوثائق الرسمية للقمة.
  - (د) إتاحة الوثائق الرسمية قبل القمة بوقت كاف.
  - (هـ) القيام بالتسجيلات الصوتية ووضع الترتيبات للاحتفاظ بها.

(و) اتخاذ الترتيبات لاستلام وثائق القمة في عدتها واحتفاظ بها، بما يتفق مع الممارسات المتبعة في الأمم المتحدة.

(ز) القيام عموماً بكل الأعمال الأخرى التي قد تتطلبها القمة.

#### المادة ١٥

##### البيانات الصادرة عن أمانة القمة

يجوز للأمين العام للقمة أو لأي عضو في أمانة القمة يسمي لهذا الغرض، رهناً بالمادة ١٩، أن يصدر في أي وقت، بإذن من الرئيس، بيانات شفوية أو مكتوبة تتعلق بأي مسألة موضع النظر.

خامساً: افتتاح القمة:

#### المادة ١٦

##### الرئيس المؤقت

يقوم الأمين العام للأمم المتحدة أو من يسميه لهذا الغرض في حالة غيابه بافتتاح الجلسة الأولى للقمة ويرأسها حتى تنتخب القمة رئيسها.

#### المادة ١٧

##### المقررات المتعلقة بالتنظيم

تقوم القمة بما يلي في جلستها الأولى:

(أ) اعتماد نظامها الداخلي.

(ب) انتخاب أعضاء مكتبها وتشكيل هيئاتها الفرعية.

(ج) اعتماد جدول أعمالها، ويكون مشروع جدول الأعمال هو جدول الأعمال المؤقت للقمة إلى حين اعتماده.

(د) البت في تنظيم أعمالها.

## المادة ١٨

### النصاب القانوني

يشترط حضور ممثلي أغلبية الدول المشاركة في القمة لاتخاذ أي قرار.

## المادة ١٩

### الكلمات

١- لا يجوز لأحد أن يخاطب القمة دون الحصول مسبقا علي إذن من الرئيس. ورهنا بالمواد ٢٠ و ٢١ ومن ٢٣ إلي ٢٦ ورهنا بالفصل الحادي عشر، عند الاقتضاء، ينادي الرئيس علي المتحدثين للحديث بالترتيب الذي أعلنوا به رغبتهم في أخذ الكلمة، وتكون أمانة القمة مسؤولة عن وضع قائمة المتحدثين.

٢- تقتصر المناقشة علي المسألة المعروضة علي القمة وللرئيس أن يوجه المتحدث إلي مراعاة النظام إذا كانت عبارات المتحدث لا تتصل بالموضوع الذي تجري مناقشته.

٣- يجوز للقمة أن تقيد الوقت المسموح به لكل متحدث وأن تقيد عدد المرات التي يجوز فيها لكل مشارك الحديث في أي مسألة. وعند تقديم اقتراح إجرائي لإعمال هذا التقييد تعطي الكلمة لاثنتين فقط من ممثلي الدول المؤيدين واثنتين من المعارضين وبعدها يعرض الاقتراح الإجرائي فورا للتصديق. وفي أي حال يقوم الرئيس بموافقة القمة بتحديد كل تدخل في الموضوعات الإجرائية بخمس دقائق. وعندما يوضع هذا الحد علي المناقشة ثم يتجاوز أحد المتحدثين الوقت المخصص يدعو الرئيس المتحدث إلي مراعاة النظام فورا.

## المادة ٢٠

### النقاط النظامية

أثناء مناقشة أي موضوع يجوز لممثل أي دولة في أي وقت أن يثير نقطة بيت فيها الرئيس فوراً وفقاً لهذا النظام الداخلي. ويجوز لممثل أي دولة أن يطعن في قرار الرئيس. ويوضع الطعن محل التصويت ويبقى حكم الرئيس سارياً إلا إذا نسخته أغلبية الممثلين الحاضرين والمصوتين. ولا يجوز لممثل يثير نقطة نظام أن يتحدث في صلب المسألة موضع المناقشة.

## المادة ٢١

### الأسبقية

يجوز إعطاء الأسبقية في قائمة المتحدثين لرئيس إحدى اللجان بغرض تفسير استنتاجات توصلت إليها الهيئة المعنية.

## المادة ٢٢

### قفل قائمة المتحدثين

يجوز للرئيس أثناء أي مناقشة أن يعلن قائمة المتحدثين وأن يعلن قفلها بموافقة القمة.

## المادة ٢٣

### حق الرد

١- رغم حكم المادة ٢٢ يعطي الرئيس حق الرد لممثل أي دولة مشاركة في القمة أو لممثل الجماعات الأوربية إذا طلب ذلك. ويجوز إعطاء أي ممثل آخر فرصة الرد.<sup>(١)</sup>

---

(١) لا يتمتع المراقبون بحق الرد.



- ٢- تلقي الكلمات التي يتم الإدلاء بها بموجب هذه المادة عادة في نهاية الجلسة الأخيرة في يوم اجتماع الهيئة المعنية أو عند نهاية النظر في البند المعني إذا كان ذلك قبل الجلسة الأخيرة.
- ٣- لا يجوز لممثلي الدول أو الجماعة الأوروبية الإدلاء بأكثر من بيانين بموجب هذه المادة في أي جلسة واحدة بشأن أي بند واحد. ويقتصر البيان الأول على خمس دقائق والبيان الثاني على ثلاث دقائق.
- ٤- تهدي البيانات الملقاة بموجب هذه المادة إلى الإيجاز قدر الإمكان.

#### المادة ٢٤

##### إرجاء المناقشة

يجوز لممثل أي دولة مشاركة في القمة أن يقترح في أي وقت إرجاء مناقشة المسألة الجارية. وبالإضافة إلى الممثل الذي يقترح هذا الإجراء، يعطي الإنز للحدث عن هذا الإجراء لاثنتين فقط من ممثلي الدول يؤيدانه واثنتين يعارضانه، وبعدها يعرض الاقتراح الإجرائي للتصويت فوراً رهنا بالمادة ٢٧.

#### المادة ٢٥

##### إغلاق المناقشة

يجوز لممثل أي دعوى مشاركة في القمة أن يقترح في أي وقت إغلاق مناقشة المسألة الجارية، سواء أعلن أو لم يعلن متحدثون آخرون عن رغبتهم في الكلام. ويعطي الإنز للحدث عن هذا الإجراء لاثنتين فقط من ممثلي الدول يعارضان إغلاق المناقشة وبعدها يعرض الاقتراح للتصويت فوراً رهنا بالمادة ٢٧.

## المادة ٢٧

### تعليق أو رفع الجلسة

يجوز لممثل أي دولة مشاركة في القمة، رهنا بالمادة ٢٧، أن يقترح في أي وقت تعليق أو رفع الجلسة. ولا يسمح بمناقشة اقتراح إجرائي من هذا القبيل، ولكنه يعرض فوراً للتصويت رهنا بالمادة ٢٧.

## المادة ٢٧

### ترتيب الاقتراحات الإجرائية

تأخذ الاقتراحات الإجرائية الموضحة أدناه الأسبقية بالترتيب التالي علي جميع المقترحات أو الاقتراحات الإجرائية والنقاط النظامية الأخرى المعروضة علي الجلسة:

(أ) تعليق الجلسة.

(ب) رفع الجلسة.

(ج) إرجاء مناقشة مسألة جارية.

(د) إغلاق مناقشة مسألة جارية.

## المادة ٢٨

### تقديم المقترحات والتعديلات

تقدم المقترحات والتعديلات الموضوعية عادة في شكل مكتوب إلي الأمين العام للقمة أو من يعين ممثلاً له، ويقوم هذا الأخير بتعميم نسخ علي جميع الوفود. ولا تناقش المقترحات الموضوعية أو تطرح لاتخاذ قرار بشأنها إلا بعد مرور ٢٤ ساعة علي تعميم نسخة منها بجميع لغات القمة علي جميع الوفود، ما لم تقرر القمة خلاف ذلك. إلا أنه يجوز للرئيس أن يسمح بمناقشة وبحث التعديلات حتى لم تكن هذه التعديلات قد عممت، أو لم يجر تعميمها إلا في اليوم نفسه.

## المادة ٢٩

### سحب المقترحات والتعديلات والاقتراحات الإجرائية

يجوز لمقدمي أي مقترح أو تعديل أو اقتراح إجرائي سحبه في أي وقت قبل اتخاذ قرار بشأنه شريطة ألا يكون قد تم إدخال تعديلات عليه. ويجوز لأي ممثل أن يعيد تقديم مقترح أو تعديل أو اقتراح إجرائي سحب بهذه الطريقة، باستثناء الحالات الأخرى المنصوص عليها في هذا النظام الداخلي.

## المادة ٣٠

### البيت في الاختصاص

أي اقتراح إجرائي مقدم من ممثل أي دولة مشاركة يطالب بالبيت في اختصاص القمة في اعتماد مقترح مقدم إليها يوضع للتصويت، رهنا بأحكام المادة ٢٧، قبل اتخاذ أي قرار بشأن المقترح المذكور.

## المادة ٣١

### إعادة النظر في المقترحات

لا يجوز إعادة النظر في أي مقترح تم اعتماده أو رفضه إلا إذا قررت القمة ذلك بأغلبية ثلثي الممثلين الحاضرين والمصوتين. ويسمح بالحديث بشأن اقتراح إجرائي لإعادة النظر لاثنتين فقط من ممثلي الدول المعارضين لإعادة النظر، وبعدها يوضع الاقتراح الإجرائي فوراً للتصويت.

سابعاً: اتخاذ القرارات:

## المادة ٣٢

### توافق الآراء

١- تبذل القمة كل جهودها لكفالة إنجاز أعمالها بتوافق الآراء.

٢- لا يقوم بمفاوضات سوى الدول الأعضاء في الأمم المتحدة أو في أي وكالة متخصصة ووفد الجماعة الأوربية.

#### **المادة ٢٣**

##### **حقوق التصويت**

لكل دولة مشاركة في القمة صوت واحد.

#### **المادة ٢٤**

##### **الأغلبية المطلوبة**

- ١- في حالة عدم وجود توافق في الآراء، تتخذ القمة قراراتها بشأن جميع هذه المسائل بأغلبية الممثلين الحاضرين والمصوتين.
- ٢- إذا انقسمت الأصوات بالتساوي، يعتبر المقترح أو التعديل أو الاقتراح الإجرائي مرفوضاً.

#### **المادة ٢٥**

##### **معني عبارة "الممثلون الحاضرون والمصوتون"**

لأغراض هذا النظام تعني عبارة "الممثلون الحاضرون والمصوتون" الممثلين الذين يصوتون سلباً أو إيجاباً. ولا يعتبر الممثلون الممتنعون عن التصويت مصوتين.

#### **المادة ٢٦**

##### **أسلوب التصويت**

- ١- باستثناء الحالات المنصوص عليها في المادة ٤٣، يجري التصويت في القمة عادة برفعه الأيدي ولكن يجوز لممثل إحدى الدول أن يطلب التصويت ببناء الأسماء، وفي هذه الحالة يجري التصويت حسب الترتيب الهجائي باللغة الإنكليزية لأسماء الدول المشاركة في القمة بدءاً بالوفد الذي

يختاره الرئيس بالقرعة. وينادي اسم كل دولة في كل تصويت ببدء الأسماء ويرد الممثل بكلمة "موافق" أو معترض" أو "ممتنع".

٢- عندما تصوت القمة بالوسائل الميكانيكية/ الإلكترونية، يستعمل التصويت غير المسجل بدلا من التصويت برفع الأيدي ويستعمل التصويت المسجل بدلا من التصويت ببدء الأسماء، ويجوز لممثل أي دولة أن يطلب تسجيلًا مسجلًا ويتم هذا التصويت بدون النداء علي أسماء الدول المشاركة في القمة إلا إذا طلب ممثل دولة ما خلال ذلك.

٣- يدرج تصويت كل دولة تشارك في تصويت ببدء الأسماء أو تصويت مسجل في أي محضر أو تقرير عن الجلسة.

#### المادة ٢٧

##### التصرف أثناء التصويت

بعد أن يعلن الرئيس بدء التصويت، لا يقطع أي ممثل عملية التصويت إلا في حالة نقطة نظام تتصل بعملية التصويت.

#### المادة ٢٨

##### تعلييل التصويت

يجوز لممثلي الدول إلقاء بيانات موجزة تقتصر علي تعلييل تصويتها قبل البدء في عملية التصويت أو بعد استكمال التصويت. وللرئيس أن يقيد الوقت المسموح به لإلقاء هذا التعلييل. ولا يأخذ ممثل دولة اشتريكت في تقديم مقترح أو اقتراح إجرائي الكلمة تعلييلا لتصويتها عليه إلا في حالة تعديله.

#### المادة ٢٩

##### تجزئة المقترحات

يجوز لممثل إحدى الدول أن يقترح البت في أجزاء أي مقترح بصفة منفصلة، ويتم التصويت علي هذا الاقتراح الإجرائي لتجزئة المقترحات إذا

اعتراض عليه أحد ممثلي الدول. ويسمح فقط لاثنتين من ممثلي الدول بأخذ الكلمة لتأييد اقتراح التجزئة ولاثنتين لمعارضته. وإذا تأيد الاقتراح الإجرائي يتم تقديم أجزاء المقترح التي تمت الموافقة عليها نتيجة ذلك إلى القمة لاتخاذ قرار بشأنها ككل. وإذا رفضت كل أجزاء منطوق المقترح يعتبر المقترح مرفوضا ككل.

#### **المادة ٤٠**

##### **التعديلات**

يعتبر أي مقترح تعديلا لمقترح آخر إذا اقتصر على إضافة شيء إليه أو حذف شيء منه أو تنقيح جزء منه. وتعتبر كلمة "مقترح" في هذا النظام الداخلي شاملة التعديلات إلا إذا تم النص على خلاف ذلك بالتحديد.

#### **المادة ٤١**

##### **ترتيب التصويت على التعديلات**

عند طلب تعديل لأي مقترح يتم التصويت على التعديل أولا. وإذا اقترح تعديلات أو أكثر لأي مقترح تصوت القمة أولا على التعديل الأبعد جوهريا عن المقترح الأصلي ثم على التعديل الذي يليه فالذي يليه قريبا، حتى يتم التصويت على جميع التعديلات. ولكن إذا كان اعتماد أحد التعديلات ينطوي بالضرورة على رفض تعديل آخر، فلا يتم التصويت على هذا التعديل الآخر. وفي حالة اعتماد تعديل أو أكثر، يتم التصويت على المقترح المعدل.

#### **المادة ٤٢**

##### **ترتيب التصويت على المقترحات**

١- إذا اتصل مقترجان أو أكثر بخلاف التعديلات بمسألة واحدة، يتم التصويت حسب ترتيب تقديمها إلا إذا قررت القمة خلال ذلك. ويجوز للقمة بعد كل تصويت على أي مقترح أن تقرر ما إن كانت تصوت على المقترح التالي أم لا.

٢- يتم التصويت علي المقترحات المنقحة حسب ترتيب تقديم المقترحات الأصلية إلا إذا كان التتقيح يختلف اختلافا جوهريا عن المقترح الأصلي. وفي هذه الحالة، يعتبر المقترح الأصلي مسحوبا ويعامل المقترح المنقح بوصفه مقترحا جديدا.

٣- أي اقتراح إجرائي يتطلب عدم اتخاذ قرار بشأن أي مقترح يعرض للتصويت قبل التصويت علي المقترح المعني.

#### **المادة ٤٣**

##### **الانتخابات**

تجري كل الانتخابات بالاقتراع السري، إلا إذا قررت القمة بدون أي اعتراض أن تسير في عملية الانتخاب دون اقتراع في حالة وجود مرشح متفق عليه أو قائمة متفق عليها.

ثامنا: الهيئات الفرعية:

#### **المادة ٤٤**

##### **اللجان**

- ١- للقمة أن تنشئ من اللجان ما تعتبره ضروريا لأداء وظائفها.
- ٢- باستثناء الحالات الأخرى التي ينص عليها هذا للنظام الداخلي، يجوز لكل دولة مشاركة في القمة وكذلك للجماعة الأوربية أن تكون ممثلة في كل لجنة.

#### **المادة ٤٥**

##### **أعضاء المكتب وتسيير العمل واتخاذ القرارات**

تطبق المواد الواردة في الفصول الثاني والسادس (باستثناء المادتين ١٨ و ٢٨) والسابع أعلاه علي أعمال اللجان حسب مقتضى الحال.

**المادة ٤٦**

**لغات القمة**

لغات القمة هي الأسبانية والإنكليزية والروسية والصينية والعربية والفرنسية.

**المادة ٤٧**

**الترجمة الشفوية**

١- تترجم الكلمات التي تلقى بإحدى لغات القمة ترجمة شفوية إلى لغات القمة الأخرى.

٢- يجوز لأحد المشاركين أن يتحدث بلغة غير لغات القمة إذا اتخذ المشارك المعني الترتيبات لكفالة الترجمة الشفوية إلى إحدى هذه اللغات.

**المادة ٤٨**

**لغات الوثائق الرسمية**

تتاح الوثائق الرسمية الصادرة عن القمة بلغات القمة.

**المادة ٤٩**

**التسجيلات الصوتية للجلسات**

يكون إعداد وحفظ التسجيلات الصوتية لجلسات القمة وفقا للممارسات المتبعة في الأمم المتحدة ولا تعد تسجيلات صوتية لجلسات أي فريق عمل، ما لم تقرر القمة خلاف ذلك.



عاشراً: الجلسات المفتوحة والمعلقة:

#### المادة ٥٠<sup>(١)</sup>

تكون الجلسات العامة للقمة ولسات أي لجنة مفتوحة ما لم تقرر الهيئة المعنية خلاف ذلك. وجميع المقررات التي تتخذها الجلسة العامة للقمة في جلسة مغلقة تعلن في جلسة مفتوحة قريبة.

#### المادة ٥٠ مكرر

تعقد جلسات المكتب واللجان الفرعية وفرق العمل، كقاعدة عامة، كجلسات مغلقة.

حادي عشر: المشاركون والمراقبون الآخرون:

#### المادة ٥١

ممثلو الكيانات والمنظمات الدولية الحكومية وغيرها من الكيانات التي تلقت دعوى دائمة من الجمعية العامة للمشاركة بصفة مراقب في دورات وأعمال جميع المؤتمرات الدولية المعقودة برعاية الجمعية العامة.

الممثلون الذين تسميهم الكيانات والمنظمات الدولية الحكومية وغيرها من الكيانات التي تلقت دعوى دائمة من الجمعية العامة للمشاركة بصفة مراقب في دورات وأعمال جميع المؤتمرات الدولية المعقودة برعاية الجمعية العامة لهم الحق في المشاركة بصفة مراقب دون الحق في التصويت في مداولات الجلسات العامة للقمة وكذلك في أي اجتماع للجان الأخرى وفرق العمل، حسب الاقتضاء.

---

(1) الاجتماعات المفتوحة للقمة يقتصر حضورها على المشاركين المسجلين حسب الأصول.

## المادة ٥٢<sup>(١)</sup>

### ممثلو الوكالات المتخصصة

يجوز للممثلين الذين تسميهم الوكالات المتخصصة المشاركة بصفة مراقب دون الحق في التصويت في مداولات الجلسات العامة للقمة وكذلك في أي اجتماع للجان الأخرى أو فرق العمل بشأن أي مسائل تدرج في نطاق أنشطة هذه الوكالات حسب الاقتضاء.

## المادة ٥٣

### ممثلو المنظمات الدولية الحكومية الأخرى

باستثناء الحالات الأخرى المنصوص عليها بالتحديد في هذا النظام الداخلي في صدد الجماعة الأوروبية، يجوز للممثلين الذين تسميهم المنظمات الدولية الحكومية المدعوة لحضور القمة المشاركة بصفة مراقب دون الحق في التصويت في مداولات الجلسات العامة للقمة وكذلك في أي اجتماع للجان الأخرى أو فرق العمل بشأن أي مسائل تدرج في نطاق أنشطة هذه المنظمات حسب الاقتضاء.

## المادة ٥٤

### ممثلو أجهزة الأمم المتحدة المهتمة

يجوز للممثلين الذين تسميهم أجهزة الأمم المتحدة المهتمة المشاركة بصفة مراقب بدون الحق في التصويت في مداولات الجلسات العامة للقمة وكذلك في أي اجتماع للجان الأخرى أو فرق العمل بشأن أي مسائل تدرج في نطاق أنشطة هذه الأجهزة حسب الاقتضاء.

(١) لأغراض المادة ٥٢ يشمل تعبير "الوكالات المتخصصة" الوكالة الدولية للطاقة الذرية، والمنظمة العالمية للسياحة، ومنظمة التجارة العالمية واللجنة التحضيرية لمنظمة معاهدة الحظر الشامل للتجارب النووية، ومنظمة حظر الأسلحة الكيميائية.

## المادة ٥٥

### ممثلو المنظمات غير الحكومية، وكيانات المجتمع المدني وقطاع الأعمال

١- يجوز للمنظمات غير الحكومية وكيانات المجتمع المدني وقطاع الأعمال المعتمدة للمشاركة في اللجان أن تسمي ممثلين لحضور الاجتماعات المفتوحة للقيمة ولجانها بصفة مراقب.

٢- بدعوى من رئيس الهيئة المعنية ورهنا بموافق هذه الهيئة، يمكن لهؤلاء المراقبين الإدلاء ببيانات شفوية بشأن مسائل لهم فيها اختصاص محدد. وإذا كان عدد طلبات الإدلاء يمثل هذه البيانات كبيرا، يطلب من المنظمات غير الحكومية وكيانات المجتمع المدني وقطاع الأعمال أن تشكل نفسها في تجمعات، وتأخذ هذه التجمعات الكلمة من خلال متحدثين باسمها.

## المادة ٥٦<sup>(١)</sup>

### الأعضاء المنتسبون في اللجان الإقليمية

يجوز للممثلين الذين يسميهم الأعضاء المنتسبون في اللجان الإقليمية المشاركة بصفة مراقب دون الحق في التصويت في مداولات الجلسات العامة للقيمة وكذلك في أي اجتماع للجان الأخرى أو فرق العمل بشأن مسائل تدرج في نطاق أنشطة هؤلاء الأعضاء حسب الاقتضاء.

## المادة ٥٧

### البيانات المكتوبة

توزع الأمانة البيانات المكتوبة المقدمة من الممثلين الذين تتم تسميتهم والمشار إليهم في المواد من ٥١ إلى ٥٦ علي جميع الوفود بالكميات

(١) أروبا، الأنتيل النيثرلندية، أنغويلا، بورتوريكو، بولينيزيا الفرنسية، الجزر العذراء الأمريكية، الجزر العذراء البريطانية، ساموا الأمريكية، غوام، كاليدونيا الجديدة، ماريانا الشمالية (كومنولث جزر..) مونسيرات.

وباللغات التي تتاح بها هذه البيانات للأمانة في موقع القمة شريطة أن يكون أي بيان مقدم باسم منظمة غير حكومية أو أي كيان من المجتمع المدني أو من قطاع الأعمال متصلاً بأعمال القمة وأن يكون عن موضوع تتمتع المنظمة غير الحكومية أو كيان المجتمع المدني أو كيان قطاع الأعمال باختصاص خاص فيه.

ثاني عشر: تعليق النظام الداخلي وتعديله:

#### المادة ٥٨

##### أسلوب التعليق

يجوز للقمة أن تعلق تطبيق أي مادة في هذا النظام الداخلي بشرط إصدار إشعار قبل اقتراح التعليق بأربع وعشرين (٢٤) ساعة ويجوز إلغاء هذا الشرط إذا لم يعترض أحد ممثلي الدول. ويقتصر هذا التعليق على غرض محدد معلن ويقتصر على الفترة التي يتطلبها تحقيق هذا الغرض.

#### المادة ٥٩

##### أسلوب التعديل

يجوز تعديل هذا النظام الداخلي بقرار من القمة يتخذ بأغلبية ثلثي الممثلين الحاضرين والمصوتين بعد أن يقدم المكتب تقريراً عن التعديل المقترح.

**التقرير الختامي للاجتماع التحضيري**  
**(الاجتماع الأول للجنة التحضيرية لمرحلة تونس)**

القمة العالمية لمجتمع المعلومات  
مركز مؤتمرات المدينة، ياسمين الحمامات،  
تونس، ٢٤ - ٢٦ يونيو ٢٠٠٤

أولاً: مقبلة.

ثانياً: التنظيم.

ألف) افتتاح الاجتماع التحضيري.

باء) انتخاب رئيس اللجنة التحضيرية.

جيم) جدول الأعمال.

دال) تعديل المادة ٩ من النظام الداخلي للجنة التحضيرية.

هـ) انتخاب نواب رئيس اللجنة التحضيرية.

واو) انتخاب أعضاء مكتب الاجتماع التحضيري الآخرين (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).

زاي) اعتماد العضوية.

حاء) تنظيم العمل.

طاء) تقرير الأمين العام للاتحاد الدولي للاتصالات عن الأنشطة السابقة  
لاجتماع اللجنة التحضيرية (الاجتماع الأول للجنة التحضيرية لمرحلة  
تونس).

ياء) الحضور.

كاف) الوثائق.

ثالثاً: تقرير ممثلي الأمين العام للأمم المتحدة بشأن فريق المهام المعني بالآليات المالية وفريق العمل المعني بإدارة الإنترنت.

رابعاً: محور اهتمام ونتائج وهيكل عملية مرحلة تونس - الترتيبات الخاصة بالاجتماع الثاني للجنة التحضيرية.

خامساً: اعتماد تقرير الاجتماع الأول للجنة التحضيرية.

سادساً: اختتام الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).

سابعاً: الملحق.

الملحق ١: قرار الاجتماع الأول للجنة التحضيرية.

## أولاً: مقدمة:

١- رحبت الجمعية العامة للأمم المتحدة في قرارها ١٨٣/٥٦ الصادر في ٢١ ديسمبر ٢٠٠١ بقرار مجلس الاتحاد الدولي للاتصالات الذي أيد المجلس فيه اقتراح الأمين العام للاتحاد الدولي للاتصالات بعقد القمة العالمية لمجتمع المعلومات في مرحلتين، مرحلة أولى تعقد في جنيف في الفترة ١٠-١٢ ديسمبر ٢٠٠٣، ومرحلة ثانية في تونس. ودعت الجمعية العامة أيضا الاتحاد الدولي للاتصالات إلى أن يضطلع بالدور القيادي في الأمانة التنفيذية للقمة وفي عملية التحضير للقمة، بالتعاون مع المنظمات والشركاء الآخرين المهتمين.

٢- وأوصت الجمعية العامة كذلك بأن يعهد بالأعمال التحضيرية للقمة إلى لجنة تحضيرية دولية حكومية مفتوحة العضوية تحدد جدول أعمال القمة، وتضع مشروع الإعلان ومشروع خطة العمل في صيغتهما النهائية، وتبث في إجراءات مشاركة أصحاب المصلحة الآخرين في القمة.

٣- وفي مرحلة جنيف من القمة العالمية لمجتمع المعلومات، ١٠-١٢ ديسمبر ٢٠٠٣، قررت الحكومات بموجب قرارها الخاص بـ "ترتيبات مرحلة تونس من القمة"، عقد اجتماع تحضيري في النصف الأول من عام ٢٠٠٣ لاستعراض قضايا مجتمع المعلومات التي ينبغي أن ينصب عليها اهتمام مرحلة تونس من القمة العالمية لمجتمع المعلومات، والاتفاق على هيكل عملية المرحلة الثانية استنادا إلى المساهمات المقدمة من الوفود. وينبغي لمكتب مرحلة تونس من القمة العالمية لمجتمع المعلومات أن يبدأ، تحت قيادة رئيسه، الإعداد لهذا الاجتماع التحضيري".

ثانيا: التنظيم:

**ألف) افتتاح الاجتماع:**

٤- عقدت اللجنة التحضيرية دورتها الأولى (وتسمى الاجتماع التحضيري - الاجتماع الأول للجنة التحضيرية لمرحلة تونس) في الفترة من ٢٤ إلى ٢٦ يونيو ٢٠٠٤ في مركز مؤتمرات المدينة في ياسمين الحمامات بتونس. وقد عقدت اللجنة ست جلسات عامة.

٥- افتتح السيد يوشيو أوتسومي الأمين العام للاتحاد الدولي للاتصالات ورئيس اللجنة الرفيعة المستوى لتنظيم القمة الجلسة العامة الأولى وترأس عملية انتخاب رئيس اللجنة التحضيرية لمرحلة تونس من القمة العالمية لمجتمع المعلومات.

**باء) انتخاب رئيس اللجنة التحضيرية:**

٦- انتخبت اللجنة التحضيرية بالإجماع صاحب السعادة السفير جانيس كاركلينز، لاتفيا، رئيسا للجنة التحضيرية لمرحلة تونس من القمة العالمية لمجتمع المعلومات.

**جيم) جدول الأعمال:**

٧- اعتمدت اللجنة التحضيرية جدول أعمال الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس) علي النحو الوارد في الوثيقة 1/ DOC/ PC-1/ WSIS-II الأعمال كما يلي:

١- افتتاح الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).

٢- انتخاب رئيس اللجنة التحضيرية.



- ٣- اعتماد جدول أعمال الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).
- ٤- تعديل المادة ٩ من النظام الداخلي للجنة التحضيرية.
- ٥- انتخاب نواب رئيس اللجنة التحضيرية.
- ٦- انتخاب أعضاء مكتب الاجتماع التحضيري الآخرين (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).
- ٧- اعتماد المنظمات غير الحكومية ومنظمات المجتمع المدني وكيانات الأعمال.
- ٨- تنظيم أعمال الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).
- ٩- تقرير الأمين العام للاتحاد الدولي للاتصالات عن الأنشطة السابقة للاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).
- ١٠- تقرير ممثل الأمين العام للأمم المتحدة عن فريق العمل المعني بإدارة الإنترنت.
- ١١- تقرير ممثل برنامج الأمم المتحدة الإنمائي عن فريق المهام المعني بالآليات المالية.
- ١٢- محور اهتمام مرحلة تونس ونتائجها.
- ١٣- هيكل عملية مرحلة تونس.
- ١٤- ترتيبات الاجتماعات المقبلة للجنة التحضيرية.
- ١٥- اعتماد تقرير الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).

١٦- أعمال أخرى.

١٧- اختتام الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس).

دال) تعديل المادة ٩ من النظام الداخلي للجنة التحضيرية:

٨- اقترح المكتب المؤقت للجنة التحضيرية لمرحلة من القمة العالمية لمجتمع المعلومات تعديل المادة ٩ من النظام الداخلي للجنة التحضيرية. ووافقت اللجنة التحضيرية علي الاستعاضة عن المادة ٩ بالنص التالي:

#### المادة ٩

##### الانتخابات

تنتخب اللجنة التحضيرية من بين ممثلي الدول المشاركة أعضاء المكتب التاليين: رئيس وتسعة وعشرون نائباً للرئيس يقوم أحدهم بعمل المقرر، علي أن يكون انتخاب هؤلاء المسؤولين علي أساس كفالة الطابع التمثيلي للمكتب، كما تنتخب نائبين للرئيس يرشحهما البلدان المضيفان للقمة بحكم استضافتهما للقمة. ويجوز للجنة التحضيرية أيضاً أن تنتخب أي أعضاء آخرين للمكتب حسبما تراه ضروريا لأداء وظائفها.

هاء) انتخاب نواب رئيس اللجنة التحضيرية:

٩- قامت اللجنة التحضيرية، بناء علي المشاورات التي أجريت مع المجموعات الإقليمية والمكتب، بانتخاب نواب الرئيس التاليين بالإجماع:

- إقليم إفريقيا: مصر، كينيا، ليبيا، مالي، السنغال، زامبيا.
- إقليم آسيا: بنغلادش، الصين، اليابان، باكستان، جمهورية كوريا، المملكة العربية السعودية.

- إقليم أوروبا الشرقية: أرمينيا، بيلاروس، هنغاريا، روسيا، الصرب والجبل الأسود.

- إقليم أمريكا اللاتينية والبحر الكاريبي: الأرجنتين، البرازيل، المكسيك، نيكاراغوا، ترينيداد وتوباغو، فنزويلا.

- إقليم أوروبا الغربية وأقاليم أخرى: كندا، فرنسا، اليونان، النرويج، إسبانيا، الولايات المتحدة الأمريكية.

- عضوان يمثلان البلدين المضيفين: سويسرا وتونس.

**واو) انتخاب أعضاء مكتب اللجنة التحضيرية الآخرين (الاجتماع الأول للجنة التحضيرية لمرحلة تونس):**

١٠- كما انتخبت اللجنة التحضيرية بالإجماع السيد جورج بابادانتوس (اليونان) مقررا.

**زاي) اعتماد العضوية:**

١١- ذكر الرئيس المشاركين بأن القمة العالمية لمجتمع المعلومات هي قمة من مرحلتين وبأن جميع الكيانات التي اعتمدت في مرحلة جنيف من القمة ستبقي معتمدة في مرحلة تونس من القمة. وأقرت اللجنة التحضيرية قائمة الكيانات التي طلبت اعتماد عضويتها بعد المرحلة الأولى، وذلك علي النحو الوارد في الوثيقة<sup>(١)</sup>.

**حاء) تنظيم العمل:**

١٢- قام الأمين التنفيذي بإحاطة المشاركين علما بجدول الأعمال المشروع<sup>(٢)</sup> ومشروع خطة إدارة الوقت<sup>(١)</sup>، وقد تم تعديل مشروع خطة إدارة الوقت بما يتفق مع القرار الذي اتخذ بشأن البند ١٠ من جدول الأعمال.

(١) WSIS- II/ PC- 1/ DOC/ 3

(٢) WSIS- II/ PC- 1/ DOC/ 3

١٣- استمعت اللجنة التحضيرية في الاجتماع الأول للجلسة العامة، يوم ٢٤ يونيو ٢٠٠٤، إلى بيانات عامة موجزة من الدول التالية: أيرلندا بالنيابة عن الاتحاد الأوروبي، اليابان، النرويج، كوريا، إسبانيا، لاتفيا، إندونيسيا، الجزائر، سورية، هايتي، البرازيل، بيلاروس، باكستان، السودان، زامبيا نيابة عن المجموعة الإفريقية، الصين وكندا.

١٤- وفي الاجتماع الثاني للجلسة العامة، يوم ٢٤ يونيو ٢٠٠٤، استمعت اللجنة التحضيرية إلى بيانات من الدول التالية: تشاد وكوبا وبوتسوانا.

طاء) تقرير الأمين العام للاتحاد الدولي للاتصالات عن الأنشطة السابقة للاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس):

١٥- قدم الأمين العام تقريراً مكتوباً عن نتائج القمة، وكذلك عن الأنشطة التي قام بها الاتحاد ومنظومة الأمم المتحدة في سبيل التحضير للاجتماع الأول للجنة التحضيرية<sup>(٢)</sup>.

#### باء) الحضور:

١٦- وفقاً للفقرة ٢ من قرار الجمعية العامة ١٨٣/٥٦ والمادة ١ من النظام الداخلي، تكون الدورة الأولى للجنة التحضيرية للقمة العالمية لمجتمع المعلومات مفتوحة أمام مشاركة جميع الدول الأعضاء في الأمم المتحدة أو في أي من وكالاتها المتخصصة.

١٧- كانت الدول المائة والسبعة والعشرون التالية أسماؤها ممثلة في اجتماع اللجنة التحضيرية: الجزاء، أندورا، أنغولا، الأرجنتين، أرمينيا، أستراليا، النمسا، أذربيجان، البحرين، بنغلاديش، بربادوس، بيلاروس، بلجيكا،

(١) WSIS- II/ PC- 1/ DOC/ 2 (١)  
(٢) WSIS- II/ PC- 1/ DOC/ 4 (2)

بسن، بوتان، بوليفيا، البوسنة والهرسك، بوتسوانا، البرازيل، بلغاريا، بوركينا فاسو، كمبوديا، الكامرون، كندا، جمهورية إفريقيا الوسطى، تشاد، شيلي، الصين، كولومبيا، جزر القمر، جمهورية الكونغو، كوت ديفوار، كرواتيا، كوبا، الجمهورية التشيكية، جمهورية الكونغو الديمقراطية، الدانمارك، الجمهورية الدومينيكية، مصر، السلفادور، إستونيا، فنلندا، فرنسا، الغابون، غامبيا، ألمانيا، غانا، اليونان، غواتيمالا، غينيا، هايتي، هانغريا، الهند، إندونيسيا، جمهورية إيران الإسلامية، العراق، أيرلندا، إسرائيل، اليابان، الأردن، كينيا، جمهورية كوريا، الكويت، لاوس، لبنان، ليسوتو، ليبيريا، ليبيا، ليتوانيا، لكسمبرغ، مدغشقر، ماليزيا، مالي، مالتة، موريتانيا، موريشيوس، المكسيك، موناكو، منغوليا، المغرب، موزامبيق، ميانمار، ناميبيا، نيبال، هولندا، نيكاراغوا، النيجر، نيجيريا، النرويج، عمان، باكستان، بنما، باراغواي، بولندا، البرتغال، روسيا، المملكة العربية السعودية، السنغال، صربيا والجبل الأسود، جمهورية سلوفاكيا، سلوفينيا، جزر سليمان، جنوب أفريقيا، إسبانيا، سري لانكا، السودان، السويد، سويسرا، سورية، تنزانيا، جمهورية مقدونيا، اليوغوسلافية السابقة، توغو، ترينيداد وتوباغو، تونس، تركيا، أوغندا، أوكرانيا، الإمارات العربية المتحدة، المملكة المتحدة، الولايات المتحدة الأمريكية، أوروغواي، الفاتيكان، فنزويلا، فيتنام، زامبيا، زيمبابوي.

١٨- كان الاتحاد الأوروبي ممثلاً في الاجتماع وفقاً للنظام الداخلي للجنة التحضيرية.

١٩- تلقت فلسطين دعوى دائمة من الجمعية العامة للأمم المتحدة، وكانت ممثلة في الاجتماع.

٢٠- كانت هيئات الأمم المتحدة التالية ممثلة في الاجتماع: مكتب مندوب الأمم المتحدة السامي لحقوق الإنسان، الأمم المتحدة، مؤتمر الأمم المتحدة للتجارة والتنمية، برنامج الأمم المتحدة الإنمائي، اللجنة الاقتصادية لإفريقيا،

اللجنة الاقتصادية لأمريكا اللاتينية والكاريبي، اللجنة الاقتصادية والاجتماعية لآسيا والمحيط الهادئ، اللجنة الاقتصادية والاجتماعية لغربي آسيا، صندوق الأمم المتحدة للسكان، مفوض الأمم المتحدة السامي لشؤون اللاجئين، معهد الأمم المتحدة للتدريب والبحث، فرقة العمل المعنية بتكنولوجيا المعلومات والاتصالات التابعة للأمم المتحدة، دائرة الاتصال مع المنظمات غير الحكومية (الأمم المتحدة)، جامعة الأمم المتحدة.

٢١- كانت وكالات الأمم المتحدة المتخصصة والمنظمات ذات الصلة التالية ممثلة في الاجتماع: منظمة العمل الدولية، الاتحاد الدولي للاتصالات، منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) الاتحاد البريدي العالمي، البنك الدولي، منظمة الصحة العالمية، المنظمة العالمية للملكية الفكرية، المنظمة العالمية للأرصاد الجوية.

٢٢- كانت المنظمات الدولية الحكومية التالية التي وجهت لها دعوى ممثلة في الاجتماع: الوكالة الدولية للفرانكفونية، بنك التنمية الإفريقي، المنظمة العربية للتربية والثقافة والعلوم، بنك التنمية الآسيوي، مركز البيئة والتنمية للإقليم العربي وأوروبا (سيداري)، رابطة الدول المستقلة، المنظمة الأوربية للبحوث النووية، بنك التنمية الأمريكي، المنظمة الإسلامية للتربية والعلوم والثقافة، المنظمة الدولية للهجرة، جامعة الدول العربية، المنظمة الدولية للفرانكفونية، منظمة التعاون والتنمية في الميدان الاقتصادي.

٢٣- وحضر الاجتماع عدد كبير من المنظمات غير الحكومية وكيانات قطاع الأعمال التجارية بما فيها أعضاء قطاعات الاتحاد الدولي للاتصالات.

#### كاف) الوثائق:

٢٤- كانت الوثائق الرسمية التالية معروضة علي الدورة الأولى للجنة التحضيرية لمرحلة تونس من القمة العالمية لمجتمع المعلومات:

- مشروع جدول الأعمال<sup>(١)</sup>.
- تعديل المادة ٩ من النظام الداخلي<sup>(٢)</sup>.
- اعتماد عضوية المنظمات غير الحكومية، وكيانات المجتمع المدني وكيانات قطاع الأعمال في القمة العالمية لمجتمع المعلومات<sup>(٣)</sup>.
- تقرير الأمين العام للاتحاد بشأن الأنشطة السابقة علي الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس من القمة)<sup>(٤)</sup>.

ويمكن الإطلاع علي هذه الوثائق علي موقع القمة العالمية لمجتمع المعلومات علي شبكة الويب في العنوان التالي:

<http://www.itu.int/wsis/documents>

**ثالثاً: تقرير ممثلي الأمين العام للأمم المتحدة بشأن فريق المهام المهني بالآليات المالية وفريق العمل المعني بإدارة الإنترنت:**

٢٥- قدم السيد نشيموتو، المدير المساعد لبرنامج الأمم المتحدة الإنمائي، ومدير مكتب السياسات الإنمائية بالبرنامج، تقريراً عن التقدم الذي حققه فريق المهام المعني بالآليات المالية، الذي أنشئ تنفيذاً لقرار مرحلة جنيف من القمة (إعلان المبادئ، الفقرة ٦١ وخطة العمل، الفقرة دال ٢ (و)). ومن المتوقع أن يجتمع فريق المهام بحلول منتصف يوليو ٢٠٠٤ وأن يصدر تقريراً مبدئياً في نوفمبر ٢٠٠٤. وسوف يوضع التقرير في شكله النهائي في شهر ديسمبر ويقدم إلي الاجتماع الثاني للجنة التحضيرية في فبراير ٢٠٠٥. ويمكن الاطلاع علي بيان السيد نشيموتو في الموقع التالي علي شبكة الويب

- 
- (1) WSIS- II/ PC- 1/ DOC/ 1
  - (2) WSIS- II/ PC- 1/ DOC/ 2
  - (3) WSIS- II/ PC- 1/ DOC/ 3
  - (4) WSIS- II/ PC- 1/ DOC/ 4

<http://www.itu.int/wsis/preparatory2/hammamet/index.html>.

٢٦- قدم السيد كرومر، المنسق التنفيذي للأمانة فريق العمل المعني بإدارة الإنترنت تقريراً عن الأعمال التي قام بها فريق العمل الذي أنشئ تنفيذاً لقرار مرحلة جنيف من القمة (إعلان المبادئ، الفقرة ٨؛ وخطة العمل، الفقرة جيم ٦-١٣ ب). وسوف تبدأ الأمانة عملها اعتباراً من أول يوليو ٢٠٠٤، وسوف يعقد سلسلة مشاورات مفتوحة لجميع الحكومات وأصحاب المصلحة بشأن تشكيل فريق العمل وهيكله في سبتمبر ٢٠٠٤. وسوف يتم تعيين أعضاء فريق العمل في أكتوبر ٢٠٠٤. وسوف يعقد فريق العمل ثلاثة أو أربعة اجتماعات، ويمكن أن تجري المشاورات المفتوحة وقت انعقاد الاجتماع الثاني للجنة التحضيرية في إبريل أو مايو ٢٠٠٥، وسوف يكون التقرير النهائي متوافراً في يوليو ٢٠٠٥، على أقصى تقدير.

ويمكن الاطلاع على بيان السيد كرومر في الموقع التالي على شبكة الويب <http://www.itu.int/wsis/preparatory2/hammamet/index.html>.

**رابعاً: محور اهتمام ونتائج وهيكل مرحلة تونس - الترتيبات الخاصة بالاجتماع الثاني للجنة التحضيرية:**

٢٧- بداية من صباح اليوم الثاني وخلال اليوم الثالث، نظرت الجلسة العامة في البند ١٢ الذي يتناول محور اهتمام مرحلة تونس ونتائجها، والبند ١٣ الذي يتناول هيكل مرحلة تونس، والبند ١٤ الذي يتناول الترتيبات الخاصة بالاجتماعات المقبلة للجنة التحضيرية. وبعد تبادل مستفيض لوجهات النظر، وزع رئيس اللجنة التحضيرية مشروع قرار كانت الحكومات قد ناقشته في فريق عمل. وقد اعتمد النص النهائي الذي وضعه فريق العمل في الجلسة العامة الأخيرة يوم ٢٦ يونيو ٢٠٠٤ وهو ملحق بهذا التقرير.



٢٨- تلي الوثيقة الاشتراطات المنصوص عليها في الفقرة ٢٩ من خطة العمل التي اعتمدت في مرحلة جنيف. وتتضمن علي وجه الخصوص قرارا بشأن محور اهتمام مرحلة تونس ونتائجها وهيكل العملية التحضيرية. كذلك تحدد الوثيقة تواريخ ومدة انعقاد الاجتماع الثاني للجنة التحضيرية وتحدد العملية الخاصة بإعداد الوثائق اللازمة للاجتماع الثاني للجنة التحضيرية. كما تتضمن الوثيقة رسماً بيانياً ("خريطة طريق") يوضح العملية التحضيرية لمرحلة تونس.

#### خامساً: اعتماد تقرير الدورة الأولى للجنة التحضيرية:

٢٩- تم اعتماد مشروع تقرير الدورة الأولى للجنة التحضيرية في الاجتماع الأخير للجلسة العامة يوم ٢٦ يونيو ٢٠٠٤، وكلف المقرر بوضع التقرير في صورته النهائية بمساعدة الأمانة التنفيذي.

#### سادساً: اختتام الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية لمرحلة تونس):

٣٠- في الاجتماع الأخير للجلسة العامة، يوم ٢٦ يونيو ٢٠٠٤، شكر البلد المضيف، في بيان ختامي، جميع المشاركين علي مساهماتهم أثناء الاجتماع التحضيري. وتحدث منسقو المناطق، نيابة عن الدول الأعضاء، معربين عن تقديرهم للحكومة التونسية لما قدمته من تسهيلات ممتازة أثناء الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية) والاستقبال الحار والحفاوة التي تمتع بها جميع المشاركين.

#### سابعاً: الملحق:

##### الملحق ١

#### قرار الاجتماع الأول للجنة التحضيرية

القمة العالمية لمجتمع المعلومات- قمة واحدة تتعقد علي مرحلتين- توفر فرصة فريدة للمجتمع الدولي لمعالجة قضايا مجتمع المعلومات في إطار

شامل جامع، وضمان أن نتاح للجميع فوائد التكنولوجيات الجديدة، لا سيما تكنولوجيا المعلومات والاتصالات، وقد اعتمدت مرحلة جنيف إعلان مبادئ وخطة عمل. وتماشيا مع القرار المتخذ في مرحلة جنيف بشأن الأعمال التحضيرية لمرحلة تونس والفقرة ٢٩ من خطة العمل، قام الاجتماع التحضيري (الاجتماع الأول للجنة التحضيرية) باستعراض المسائل التي تتصل بمجتمع المعلومات والتي ينبغي أن تركز عليها المرحلة الثانية للقمة في تونس والاتفاق على الهيكل التالي للعملية التحضيرية للمرحلة الثانية:

**ألف: محور اهتمام مرحلة تونس ونتائجها وعملياتها التحضيرية:**

- (١) ينبغي أن ينصب اهتمام مرحلة تونس على ما يلي:
  - متابعة وتنفيذ إعلان المبادئ وخطة عمل جنيف من قبل أصحاب المصلحة على المستويات الوطنية والإقليمية والدولية مع اهتمام خاص بالتحديات التي تواجهها أقل البلدان نموا.
  - النظر في تقرير فريق المهام المعني بالآليات المالية (TFFM) واتخاذ الإجراءات المناسبة.
  - إدارة الإنترنت: النظر في تقرير فريق العمل المعني بإدارة الإنترنت (WGIG) واتخاذ الإجراءات المناسبة.
- (٢) ينبغي عدم إعادة فتح باب النقاش في الاتفاقات التي سبق التوصل إليها في جنيف.
- (٣) ينبغي أن تسفر مرحلة تونس عن وثيقة أو وثائق نهائية، تتكون من جزء سياسي موجز وجزء تشغيلي، كلاهما يوضحان محور اهتمام مرحلة تونس ويؤكدان بل يدعمان الالتزامات التي تم التعهد بها في مرحلة جنيف.

٤) ينبغي أن تكون العملية التحضيرية لمرحلة تونس شاملة وشفافة وفعالة من حيث التكلفة، وأن تتسم بالكفاءة، وأن تتبع من حيث المبدأ خريطة الطريق الموضحة في الشكل الوارد في الملحق.

#### باء- الاجتماع الثاني للجنة التحضيرية:

- ١) يقوم فريق أصدقاء رئيس اللجنة التحضيرية لمرحلة تونس، بمساعدة من الأمانة التنفيذية للقمة العالمية لمجتمع المعلومات، وبالتشاور مع المجموعات الإقليمية، بإعداد وثيقة تستخدم كأساس للتفاوض في الاجتماع الثاني للجنة التحضيرية، وتراعى عند اللزوم نتائج الاجتماعات المواضيعية والإقليمية وغيرها من الاجتماعات المتصلة بالقمة، حسب مقتضى الحال.
- ٢) يعقد الاجتماع الثاني للجنة التحضيرية في جنيف، لمدة سبعة أيام عمل اعتباراً من ١٧ فبراير ٢٠٠٥.



**التقرير النهائي للاجتماع التحضيري**  
**(الاجتماع الثاني للجنة التحضيرية لمرحلة تونس)**  
**القمة العالمية لمجتمع المعلومات**  
**المحتويات**

أولاً: مقدمة	
ثانياً: التنظيم	
ألف افتتاح الاجتماع ومدته	
باء جدول الأعمال وتنظيم العمل	
جيم انتخاب رئيس اللجنة الفرعية والمقرر	
دال اعتماد المشاركين	
هاء تقرير الأمين العام للاتحاد الدولي للاتصالات عن الأنشطة السابقة على الاجتماع الثاني للجنة التحضيرية.	
واو تقديم التقارير عن الأنشطة المتصلة مباشرة بالقمة	
أ) تقرير محلي عن التقييم	
ب) تقرير فريق أصدقاء رئيس اللجنة التحضيرية	
ج) تقرير فريق المهام المعني بالآليات المالية	
د) تقرير أولى لفريق العمل المعني بإدارة الانترنت	
هـ) تقارير المؤتمرات الإقليمية الاجتماعات الموضوعية	
زاي الحضور	
حاء الوثائق	
ثالثاً: النظر في البنود التالية من الوثيقة ( الوثائق ) الختامية:	

أ) نص الاستهلال السياسي.

ب) نص الجزء التشغيلي

ج) أى مسائل أخرى متصلة بالوثيقة الختامية

رابعاً: تعديل المادة ٧ من النظام الداخلى للقمة

خامساً: تنظيم أعمال مرحلة تونس من القمة

سادساً: ترتيبات الاجتماع الثالث للجنة التحضيرية لمرحلة تونس

سابعاً : مسائل أخرى

ثامناً: اعتماد تقرير الاجتماع الثاني للجنة التحضيرية لمرحلة تونس

تاسعاً: الملحق

#### **الملحق ١: تقرير اللجنة الفرعية**

##### **أولاً: مقدمة**

١- رحبت الجمعية العامة للأمم المتحدة في قرارها ١٨٣/٥٦ المؤرخ في ٢١ ديسمبر ٢٠٠١ بقرار مجلس الاتحاد الدولي للاتصالات الذى أيد فيه المجلس الاقتراح الذى قدمه الأمين العام للاتحاد الدولي للاتصالات بعقد القمة العالمية لمجتمع المعلومات على مرحلتين : الأولى فى جنيف من ١٠ إلى ١٢ ديسمبر ٢٠٠٣ والثانية فى تونس. ودعت الجمعية العامة أيضاً الاتحاد الدولي للاتصالات إلى الاضطلاع بالدور الإدارى الرائد فى الأمانة التنفيذية للقمة وفى عملياتها التحضيرية، وذلك بالتعاون مع المنظمات والشركاء الآخرين المهتمين.

٢- وأوصت الجمعية العامة كذلك بأن تجرى الأعمال التحضيرية للقمة من خلال لجنة تحضيرية دولية حكومية مفتوحة العضوية تحدد جدول أعمال

القمة، وتضع مشروع الإعلان ومشروع خطة العمل في صيغتها النهائية، وتبث في إجراءات مشاركة أصحاب المصلحة الآخرين في القمة.

٣- وعقد الاجتماع الأول للجنة التحضيرية لمرحلة تونس في الحمامات بتونس من ٢٤ إلى ٢٦ يونيو ٢٠٠٤. وفي الوثيقة المعنونة " قرار الاجتماع الأول للجنة التحضيرية " ( الوثيقة WSIS-II/PC- 1/DOC/5) قررت الحكومات أن تعقد الاجتماع الثاني للجنة التحضيرية في جنيف لمدة سبعة أيام عمل تبدأ في ١٧ فبراير ٢٠٠٥.

ثانيا: التنظيم

ألف : افتتاح الاجتماع ومنتته

٤- عقدت اللجنة التحضيرية لمرحلة تونس من القمة العالمية لمجتمع المعلومات اجتماعها الثاني من ١٧ إلى ٢٥ فبراير ٢٠٠٥ في قصر الأمم بجنيف. وعقدت اللجنة خمس جلسات عامة و ١٤ جلسة للجنة الفرعية.

٥- وألقى الكلمات الافتتاحية معالي السيد منتصر عويلى، وزير تكنولوجيا الاتصالات ( تونس) ومعالي السيد موريس لوينبرغر نائب رئيس الاتحاد السويسرى ووزير البيئة والنقل والطاقة والاتصالات، والسيد يوشيو أوتسومي الأمين العام للاتحاد الدولي للاتصالات. وتوجد الكلمات الافتتاحية في موقع القمة على شبكة الويب: [www.itu.int/wsisis/documents](http://www.itu.int/wsisis/documents).

٦- وبعد حفل الافتتاح افتتح رئيس اللجنة التحضيرية سعادة السفير جانيس كاركلير للجلسة العامة الأولى.

ب) جدول الأعمال وتنظيم العمل

٧- اعتمدت اللجنة التحضيرية جدول أعمال الاجتماع الثاني للجنة التحضيرية لمرحلة تونس الوارد في الوثيقة WSIS-II/PC-2/DOC/1 وكان جدول الأعمال على النحو التالي:

- ١- إقرار جدول الأعمال والمسائل التنظيمية الأخرى.
- ٢- انتخاب رئيس للجنة الفرعية والمقرر.
- ٣- اعتماد المنظمات غير الحكومية وكيانات المجتمع المدني وقطاع الأعمال.
- ٤- تقرير الأمين العام للاتحاد عن الأنشطة الجارية بعد الاجتماع الأول للجنة التحضيرية.
- ٥- تقديم التقارير عن الأنشطة المتصلة مباشرة القمة.
  - أ) تقرير مرحلي عن تقييم القمة العالمية لمجتمع المعلومات.
  - ب) تقرير فريق أصدقاء رئيس اللجنة التحضيرية
  - ج) تقرير فريق المهام المعني بالأكليات المالية
  - د) التقرير الأولي لفريق العمل المعني بإدارة الإنترنت.
  - هـ) تقارير عن المؤتمرات الإقليمية.
  - و) تقارير عن الاجتماعات الموضوعية
- ٦- للنظر في البنود التالية من الوثيقة ( الوثائق ) الختامية:
  - أ) نص الاستهلال السياسي
  - ب) نص الجزء التشغيلي
  - ج) أى مسائل أخرى متصلة بالوثيقة ( الوثائق ) الختامية.
- ٧- تعديل المادة ٧ من النظام الداخلي للقمة.
- ٨- تنظيم أعمال مرحلة تونس من القمة.
- ٩- ترتيبات الاجتماع الثالث للجنة التحضيرية لمرحلة تونس.
- ١٠- اعتماد تقرير الاجتماع الثاني للجنة التحضيرية لمرحلة تونس.
- ١١- مسائل أخرى.



بما في ذلك: قيام أصحاب المصلحة عن الأصعدة الوطنية والإقليمية والدولية بمتابعة وتنفيذ إعلان المبادئ وخطة العمل الصادرين في جنيف، والنظر في تقرير فريق المهام المعني بالآليات واتخاذ الإجراء الملائم بشأنه؛ وأشكال متابعة عملية القمة العالمية لمجتمع المعلومات.

٨- وأبلغ رئيس اللجنة التحضيرية المشاركين بجدول الأعمال المشروح (الوثيقة II/PC-2/ADM/7) ومشروع خطة تنظيم الوقت (الوثيقة WSIS-II/PC-2/ADM/2).

#### جيم : انتخاب رئيس اللجنة الفرعية والمقرر

٩- انتخبت اللجنة التحضيرية بالتركية سعادة السفيرة إيليانا دي جيوفان (الأرجنتين) رئيساً للجنة الفرعية والكنتور جورج بابادلتوس (اليونان) مقررًا للاجتماع الثاني للجنة التحضيرية لمرحلة تونس من القمة.

#### دال: اعتماد المشاركين

١٠- وافقت اللجنة التحضيرية على القوائم التي تتضمنها (الوثيقة WSIS-II/PC-2/DOC/10) وتشمل أسماء كيانات المجتمع المدني والقطاع الخاص التي قدمت طلبات اعتمادها في الفترة بين الاجتماع الأول والاجتماع الثاني للجنة التحضيرية.

هاء: تقرير الأمين العام للاتحاد الدولي للاتصالات السابقة للاجتماع الثاني للجنة التحضيرية

١١- قدم الأمين العام تقريراً مكتوباً عن الأنشطة التي جرت في الاتحاد ومنظومة الأمم المتحدة للتحضير للاجتماع الثاني للجنة التحضيرية (الوثيقة WSIS-II/PC-2/DOC/2). ولاحظ الأمين العام في عرضه أن الأعمال التحضيرية لقمة تونس تسير على نحو طيب. واستكمل تقريره المكتوب بإعلانه تأكيد عدد من المساهمات المالية الجديدة لدعم الأنشطة التحضيرية لقمة تونس،

وبذلك بلغ مجموع المبالغ المقدمة أكثر من ٢,٧ مليون فرنك سويسرى أو ٥٥% من المبلغ المطلوب (الوثيقة (WSIS-II/PC-2/DOC/2 (add.1)). وأخذ عدد من الوفود الكلمة للإعلان عن مساهمات إضافية.

ولو: تقديم التقارير عن الأنشطة المتصلة مباشرة بالقيمة

١٢- استمعت اللجنة التحضيرية إلى التقارير التالية:

(أ) تقرير مرحلى عن التقييم (الوثيقة (WSIS-II/PC-2/DOC/6)). وعرض لكتاتور تسيم كيلي، من الأمانة التنفيذية للقيمة العالمية/الاتحاد الدولي للاتصالات هذا التقرير المرحلى فى الجلسة العامة الأولى.

(ب) تقرير فريق أصدقاء رئيس اللجنة التحضيرية (الوثيقة -WSIS-II/PC-2/DOC/3)). وعرض رئيس اللجنة التحضيرية هذا التقرير والملحقين المرفقين به. وشرح قائلاً إن الملحقين يمثلان نتيجة عدة اجتماعات عقدها فريق أصدقاء الرئيس (بما فى ذلك اجتماعات مفتوحة أمام جميع أصحاب المصلحة). وقبلت اللجنة التحضيرية الملحقين كأساس للمفاوضات فى إطار البند ٦ من جدول الأعمال.

(ج) تقرير فريق المهام المعنى بالآليات المالية (الوثيقة -WSIS-II/PC-2/DOC/7)). وعرض هذا التقرير فى الجلسة العامة الثانية السيد شوجى نيشيموتو، مساعد مدير برنامج الأمم المتحدة الإنمائى ومدير مكتب سياسات التنمية فى البرنامج. وجرى مناقشة عامة بشأن التقرير بعد عرضه.

(د) تقرير أولى لفريق العمل المعنى بإدارة الإنترنت (الوثيقة -WSIS-II/PC-2/DOC/5)). وفى الجلسة العامة الثالثة قام الأمين التنفيذى لفريق العمل بإدارة الإنترنت بعرض التقرير الأولى لفريق العمل نيابة عن رئيس الفريق السيد نيتين ديساى. وجرى مناقشة عامة بشأن التقرير الأولى بعد عرضه.

هـ) تقارير المؤتمرات الإقليمية والاجتماعات الموضوعية. استمعت اللجنة التحضيرية إلى تقارير عن المؤتمرات والاجتماعات التالية:

#### المؤتمرات الإقليمية:

مؤتمر غربي آسيا الإقليمي، ٢٢-٢٣ نوفمبر ٢٠٠٤، دمشق، الجمهورية العربية السورية، قدمته اللجنة الاقتصادية والاجتماعية لغربي آسيا. المؤتمر الإقليمية الإفريقي، ٢-٤ فبراير ٢٠٠٥، أكرا، غانا، قدمته اللجنة الاقتصادية لأمريكا.

مؤتمر بشكيك- موسكو الإقليمي الثاني عن مجتمع المعلومات، ١٦-١٨ نوفمبر ٢٠٠٤، بشكيك، قيرغيزستان، قدمه الاتحاد الروسي.

#### الاجتماعات الموضوعية:

الاجتماع الموضوعي بشأن الرساء الاقتصادية، ٧-٩ يوليو ٢٠٠٤، جنيف، سويسرا، قدمه الاتحاد الدولي للاتصالات.

تكنولوجيا المعلومات والقانون ( حكومة جمهورية بيلاروس/ اليونسكو/ الأمم المتحدة/ مكتب برنامج الأمم المتحدة الإنمائي)، ٢٨-٢٩ أكتوبر ٢٠٠٤، منسك، جمهورية بيلاروس، قدمته جمهورية بيلاروس.

دور ومكان وسائط الإعلام في مجتمع المعلومات في إفريقيا والدول العربية ( حكومة المغرب/ أوريكوم)، ٢٢-٢٤ نوفمبر ٢٠٠٤، مراكش، المغرب، قدمته اليونسكو.

دورة القمة العالمية لمجتمع المعلومات ( لجنة بيانات العلم والتكنولوجيا التابعة للمجلس الدولي للعلوم)، ١٠ نوفمبر ٢٠٠٤، برلين، ألمانيا، قدمته CODATA؛

مؤتمر تكنولوجيا المعلومات والاتصالات العالمي ٢٠٠٤، " الفجوة الرقمية واقتصاد المعرفة: مشاكل وحلول" ( حكومة أذربيجان/ منحة القمة

العالمية/ برنامج الأمم المتحدة الإنمائي)، باكو، أذربيجان، ٢٥-٢٨ نوفمبر ٢٠٠٤، قدمته أذربيجان.

الأثار الاقتصادية والاجتماعية لتكنولوجيا المعلومات والاتصالات ( منظمة العمل الدولية/ مركز التجارة الدولية/ منظمة للتعاون والتنمية في الميدان الاقتصادي / الأونكتاد)، أنتيغا، غواتيمالا، ١٧-١٩ يناير ٢٠٠٥، قدمته غواتيمالا.

مؤتمر بشكيك عن مجتمع المعلومات والتعاون الإقليمي في تكنولوجيا المعلومات والاتصالات لأغراض التنمية (حكومة قيرغيزستان/ اللجنة الاقتصادية لأوروبا/ اللجنة الاقتصادية والاجتماعية لآسيا والمحيط الهادئ/ برنامج الأمم المتحدة الإنمائي/ فرقة العمل المعنية بتكنولوجيا المعلومات والاتصالات التابعة للأمم المتحدة)، ١٦-١٨ نوفمبر ٢٠٠٤، بشكيك، قدمته جمهورية قيرغيزستان.

تطبيقات تكنولوجيا المعلومات والاتصالات في تقليل الكوارث الطبيعية، ٢١ يناير ٢٠٠٥، كوبي، اليابان، قدمته المنظمة العالمية للأرصاد الجوية. المؤتمر الدولي المعني بحرية التعبير في الفضاء السيبراني، ٣-٤ فبراير ٢٠٠٥، باريس، فرنسا، قدمته اليونسكو.

قياس مجتمع المعلومات (الأونكتاد/ منظمة التعاون والتنمية في الميدان الاقتصادي/ الاتحاد الدولي للاتصالات/ معهد اليونسكو الإحصائي/ اللجان الإقليمية للأمم المتحدة/ فرقة العمل المعنية بتكنولوجيا المعلومات والاتصالات التابعة للأمم المتحدة / البنك الدولي)، ٧-٩ فبراير ٢٠٠٥، جنيف، سويسرا، قدمته فنلندا.

"منتدى الأعمال الإلكترونية لأمريكا الجنوبية الذي عقده مركز التجارة الدولية" ( مركز التجارة الدولية/ الغرفة البرازيلية للتجارة الإلكترونية/

حكومة البرازيل)، نوفمبر ٢٠٠٤، ساو باولو، البرازيل، قدمه مركز التجارة الدولية.

نيكاراغوا نيابة عن مجموعة بلدان أمريكا اللاتينية والكاريبي قدمت عرضاً عن المؤتمر الإقليمي القادم بشأن القمة العالمية لمجتمع المعلومات، ٨ - ١٠ يونيو ٢٠٠٥، ريو دي جانيرو، البرازيل.

#### زاي : الحضور

١٣- وفقاً للفقرة ٢ من قرار الجمعية العامة ١٨٣/٥٦ والمادة ١ من النظام الداخلي للجنة التحضيرية كان الاجتماع الثاني للجنة التحضيرية للمرحلة الثانية مفتوحاً للمشاركة الكاملة من جانب جميع الدول الأعضاء في الأمم المتحدة أو في أى من وكالاتها المتخصصة.

١٤- وكانت الدول التالية، وعددها ١٤٩ دولة، ممثلة في الاجتماع: أفغانستان، البانيا، الجزائر، أندورا، أنغولا، الأرجنتين، أرمينيا، أستراليا، النمسا، أذربيجان، البحرين، بنغلاديش، بربادوس، بيلاروس، بلجيكا، بنن، بوليفيا، البوسنة والهرسك، بوتسوانا، البرازيل، بروني دار السلام، بلغاريا، بوركينا فاسو، بوروندي، كمبوديا، الكامبيرون، كندا، تشاد، شيلي، الصين، كولومبيا، جزر القمر، الكونغو (جمهورية)، كوستاريكا، كوت ديفوار، كرواتيا، كوبا، الجمهورية التشيكية، جمهورية الكونغو الديمقراطية، الدانمارك، جيبوتي، الجمهورية النومينكية، إكوادور، مصر، السلفادور، إيرستريا، إستونيا، إثيوبيا، فنلندا، فرنسا، غابون، غامبيا، ألمانيا، غانا، اليونان، غواتيمالا، غينيا، هايتي، هندوراس، هنغاريا، أيسلندا، الهند، إندونيسيا، إيران (جمهورية- الإسلامية)، العراق، أيرلندا، إسرائيل، إيطاليا، جامايكا، اليابان، الأردن، كينيا، كوريا (جمهورية)، الكويت، قيرغيزستان، لاوس، لبنان، ليسوتو، ليبيا، ليتوانيا، لكسمبرغ، ملاوى، ماليزيا، ملديف،

مالي، مالطة، موريتانيا، موريشيوس، المكسيك، ميكرونيزيا، مولدوفا،  
موناكو، منغوليا، المغرب، موزامبيق، ميانمار، ناميبيا، نيبال، هولندا،  
نيوزيلندا، نيكاراغوا، النيجر، نيجيريا، النرويج، عمان، باكستان، بنما،  
باراغواي، بيرو، الفلبين، بولندا، البرتغال، قطر، رومانيا، روسيا، رواندا،  
ساموا، المملكة العربية السعودية، السنغال، صربيا والجبل الأسود،  
سنغافورة، الجمهورية السلوفاكية، سلوفينيا، جنوب إفريقيا، إسبانيا، سرى  
لانكا، السودان، السويد، سويسرا، الجمهورية العربية السورية، تنزانيا،  
تايلاند، توغو، ترينيداد وتوباغو، تونس، تركيا، أوغندا، أوكرانيا، الإمارات  
العربية المتحدة، الولايات المتحدة الأمريكية، أوروغواي، أوزبكستان،  
الغاتيكان، فنزويلا، فيتنام، اليمن، زامبيا، زيمبابوي.

١٥- وكانت الجماعة الأوروبية ممثلة وفقاً للنظام الداخلي للجنة  
التحضيرية.

١٦- وكانت فلسطين ممثلة، حيث إن لديها دعوة دائمة من الجمعية  
العامة للأمم المتحدة.

١٧- وكانت هيئات الأمم المتحدة التالية ممثلة: مركز التجارة الدولية،  
برنامج الأمم المتحدة المشترك بشأن فيروس نقص المناعة البشرية المكتسب/  
الإيدز؛ مفوضية الأمم المتحدة لحقوق الإنسان، الأمم المتحدة، مؤتمر الأمم  
المتحدة للتجارة والتنمية (الأونكتاد)، برنامج الأمم المتحدة الإنمائي، اللجنة  
الاقتصادية لإفريقيا، اللجنة الاقتصادية لأوروبا، اللجنة الاقتصادية لأمريكا  
اللاتينية والكاريبي، برنامج الأمم المتحدة للبيئة، اللجنة الاقتصادية  
والاجتماعية لآسيا والمحيط الهادي، لجنة الأمم المتحدة الاقتصادية  
والاجتماعية لغربي آسيا، صندوق الأمم المتحدة للسكان، برنامج الأمم  
المتحدة للمستوطنات البشرية، معهد الأمم المتحدة للتدريب والبحث، فرقة

العمل المعنية بتكنولوجيا المعلومات والاتصالات التابعة للأمم المتحدة، خدمة الاتصال غير الحكومية للأمم المتحدة، جامعة الأمم المتحدة.

١٨- وكانت وكالات الأمم المتحدة المتخصصة والمنظمات المتصلة التالية ممثلة: منظمة الأمم المتحدة للأغذية والزراعة، الصندوق الدولي للتنمية الزراعية، منظمة العمل الدولية، الاتحاد الدولي للاتصالات، منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)، الاتحاد البريدي العالمي، البنك الدولي، منظمة الصحة العالمية، المنظمة العالمية للملكية الفكرية، المنظمة العالمية للأرصاد الجوية.

١٩- وكانت المنظمات الدولية الحكومية المدعوة التالية ممثلة: اتحاد الاتصالات الإفريقي، الاتحاد الإفريقي، منظمة الجامعة العربية للتربية والثقافة والعلم، بنك التنمية الآسيوي، اتحاد الاتصالات لآسيا-المحيط الهادئ، مجتمع الكاريبي، المنظمة الأوروبية للأبحاث النووية، جماعة البلدان الناطقة بالبرتغالية، منظمة اتصالات الكمنولث، مجلس أوروبا، مجلس الاتحاد الأوروبي، وكالة الفضاء الأوروبية، بنك التنمية للبلدان الأمريكية، اللجنة الدولية للصليب الأحمر، الاتحاد البرلماني الدولي، البنك الإسلامي للتنمية، المنظمة الإسلامية للتربية والعلم والثقافة، المنظمة الدولية للهجرة، جامعة الدول العربية، المنظمة الدولية للفرانكوفونية، منظمة التعاون والتنمية في الميدان الاقتصادي، منظمة المؤتمر الإسلامي، أمانة منتدى جزر المحيط الهادئ، الاتحاد البريدي للبلدان الإفريقية، شبكة أمريكا اللاتينية لتكنولوجيا المعلومات، أمانة الأيبيري الأمريكي، جماعة فرسان مالطة، الاتحاد اللاتيني.

٢٠- وحضر الدورة عدد كبير من المنظمات غير الحكومية وكيانات قطاع الأعمال بما فيها أعضاء قطاعات الاتحاد الدولي للاتصالات.

## حاء: الوثائق

٢١- عرضت الوثائق الرسمية التالية على الاجتماع الثاني للجنة التحضيرية لمرحلة تونس من القمة:

- مشروع جدول الأعمال (WSIS-II/PC-2/DOC/1).
- تقرير الأمين العام للاتحاد الدولي للاتصالات عن الأنشطة السابقة للاجتماع التحضيري (WSIS-II/PC-2/DOC/2).
- تقرير فريق أصدقاء الرئيس (WSIS-II/PC-2/DOC/3).
- النسخ المفتوح لمرحلة تونس من القمة (WSIS-II/PC-2/DOC/4).
- التقرير الأولي لفريق العمل المعني بإدارة الانترنت (WSIS-II/PC-2/DOC/5).
- التقرير المرحلي بشأن التقييم (WSIS-II/PC-2/DOC/6).
- تقرير فريق المهام المعني بالآليات المالية (WSIS-II/PC-2/DOC/7).
- تعديل المادة ٧ من النظام الداخلي للقمة (WSIS-II/PC-2/DOC/8).
- مشروع جدول أعمال مرحلة تونس من القمة (WSIS-II/PC-2/DOC/9).
- اعتماد المنظمات غير الحكومية وكيانات المجتمع المدني وقطاع الأعمال في القمة (WSIS-II/PC-2/DOC/10).

٢٢- وفي الاجتماع الأول للجنة الفرعية قدم رئيس اللجنة التحضيرية الوثيقة المعنونة "الإضافة ١ للتقرير عن أعمال فريق أصدقاء الرئيس" (الوثيقة -WSIS-II/PC-2/DOC/3 (add.1)). وتم إصدار عدد من الوثائق المؤقتة في اللجنة الفرعية.

٢٣- ويمكن الإطلاع على هذه الوثائق في موقع القمة في شبكة الويب في العنوان التالي: [www.itu.int/wsisis/documents](http://www.itu.int/wsisis/documents)



ثالثاً: النظر في البنود التالية من الوثيقة ( الوثائق) الختامية

(أ) نص الاستهلال السياسي.

(ب) نص الجزء التشغيلي

(ج) أى مسائل أخرى متصلة بالوثيقة الختامية

بما فى ذلك: قيام أصحاب المصلحة على الأصعدة الوطنية والإقليمية والدولية بمتابعة وتنفيذ إعلان المبادئ وخطة العمل الصادرين فى جنيف، والنظر فى تقرير فريق المهام المعني بالآليات المالية واتخاذ الإجراء الملزم بشأنه، وأشكال متابعة عملية القمة العالمية لمجتمع المعلومات.

٢٤- اجتمعت اللجنة الفرعية برئاسة السفيرة إليانا دى جيوفان (الأرجنتين) ١٤ مرة فى جلسات كاملة وكفريق صياغة لمناقشة مشاريع نصوص الوثيقة ( الوثائق) الختامية لمرحلة تونس استناداً إلى تقرير فريق أصدقاء رئيس اللجنة التحضيرية (WSIS-II/PC-2/DOC/3). وتم الاستماع إلى بيانات المراقبين فى بدلية كل جلسة صباحية لمدة خمس وأربعين دقيقة تقريباً.

٢٥- وبناء على المدخلات والمساهمات المكتوبة من الوفود وأصحاب المصلحة، أعدت للرئيسة، بمساعدة من الأمانة التنفيذية للقمة، مجموعة المقترحات المتعلقة بالاستهلال السياسي (DT/4) والفصل الرابع ( الطريق إلى المستقبل) من الجزء التشغيلي (DT/5) والفصل الأول من الجزء التشغيلي ((DT-2( Rev.1)). وعلاوة على ذلك دعا الرئيس الأمين العام إلى أن يقدم مقترحات بشأن آلية التنفيذ المحتملة ((DT-3 ( Rev.1)).

٢٦- قامت الرئيسة بإعداد مقترحات للتجميع بمساعدة الأمانة التنفيذية للقمة، بشأن الفصل الثانى من الجزء التشغيلي ( الآليات المالية) (DT-1) ( الجزء 2,1) بالإضافة إلى مشروع جديد للنص المتداول ( بالإضافة إلى الوثيقة-WSIS-II/PC-2/DOC/3(Rev.1) .

٢٧- أنشئت ٤ أفرقة عمل مفتوحة لجميع الدول والمراقبين لتدارس فقرات معينة في الفصل الثاني من الجزء التشغيلي. وترد نتائج هذه المناقشات في تقرير اللجنة الفرعية.

٢٨- أرفق تقرير اللجنة الفرعية بهذا التقرير، ويمكن الاطلاع على جميع وثائق العمل الأخرى المذكورة أعلاه في موقع القمة على شبكة الويب: [www.itu.int/wsis](http://www.itu.int/wsis)

( سيضع المقرر النص النهائي)

رابعاً: تعديل المادة ٧ من النظام الداخلي للقمة

( سيضع المقرر النص النهائي)

خامساً: تنظيم أعمال مرحلة تونس من القمة

( سيضع المقرر النص النهائي)

سلسلاً: ترتيبات الاجتماع الثالث للجنة التحضيرية لمرحلة تونس

( سيضع المقرر النص النهائي)

سابعاً: مسائل أخرى

( سيضع المقرر النص النهائي)

ثامناً: اعتماد تقرير الاجتماع الثاني للجنة التحضيرية لمرحلة تونس

اعتمد مشروع تقرير الاجتماع الثاني للجنة التحضيرية لمرحلة تونس في

الجلسة العامة الأخيرة المعقودة يوم ٢٥ فبراير ٢٠٠٥. وتم تكليف المقرر بوضع التقرير في صيغته النهائية بدعم من الأمانة التنفيذية.

تساعاً: الملحق

الملحق ١: تقرير اللجنة الفرعية





**سابعاً**

**قرارات القمة العربية**

**بشأن تكنولوجيا المعلومات والاتصالات**

**لمواجهة الثورة العلمية والتقنية الراهنة**



**قرارات القمة العربية**  
**بشأن تكنولوجيا المعلومات والاتصالات**  
**لمواجهة الثورة العلمية والتقنية الراهنة**

أن مجلس جامعة الدول العربية علي مستوى القمة بعد اطلاعه:

- علي منكرة جمهورية مصر العربية رقم ٤٢٦ + ٣ المؤرخة ٣/١٠/٢٠٠١.
- وعلي نتائج أعمال الدورة الخامسة لمجلس وزراء الاتصالات العربي ومكتبه التنفيذي (الدورة الاستثنائية) / القاهرة ٢١-٢٢/٢/٢٠٠١.
- وعلي قرار مجلس الجامعة رقم ٦٠٥٢ الصادر في الدورة ١١٥ المنعقدة بالقاهرة بتاريخ ١٢/٣/٢٠٠١.
- وعلي نص المادة الثامنة من معاهدة الدفاع المشترك والتعاون الاقتصادي بين دول الجامعة العربية.
- وعلي مداولات وتوصيات الدورة الاستثنائية للمجلس الاقتصادي والاجتماعي المنعقدة بعمان يوم ٢٣/٣/٢٠٠١.
- واقتناعا بالأهمية المتصاعدة لتكنولوجيا المعلومات والاتصالات في تحقيق التنمية وزيادة القدرات التنافسية للدول.
- وتحقيقا لإقامة تعاون عربي في مجال تكنولوجيا المعلومات والاتصالات، يصل بالدول العربية إلي تطوير قدراتها الذاتية، وامتلاك أدوات التقدم في المستقبل، ومن خلال حجم اقتصادي للعمل بدعم الابتكار ويضمن الجدوى الاقتصادية، ويدعم التنمية الاقتصادية والاجتماعية.

#### يقرر:

١- إيلاء مسألة تطوير القدرات العربية في مجال تكنولوجيا المعلومات والاتصالات أولوية، واعتبارها مجالا حيويا للتعاون والتنسيق علي المستوى العربي.

٢- اعتماد وثيقة الاستراتيجية العربية لمجتمع الاتصالات والتقنية المعلوماتية والتي اقراها مجلس وزراء الاتصالات العرب ويكلف المجلس ببلورتها في برامج عمل وأنشطة قابلة للتنفيذ.

٣- أن يكون مجلس وزراء الاتصالات العرب هو الهيئة التنفيذية العليا لتنمية مجتمع الاتصالات وتقنية المعلومات العربي وتعديل الفقرة ٤ من المادة الثالثة من النظام الأساسي للمجلس الصادر به قرار المجلس الاقتصادي والاجتماعي رقم ١٠٨٦ وقرار مجلس الجامعة رقم ٥١٩٣. بما ينسجم وذلك.

٤- إنشاء "المنتدى العربي لتكنولوجيا المعلومات" تكون عضويته بالانضمام من الحكومات والقطاع الخاص ومراكز الأبحاث المعنية بقطاع تكنولوجيا المعلومات والاتصالات وتكون مهمته العمل علي دعم الأنشطة الجديدة لمجلس وزراء الاتصالات العرب من خلال:

أ- رفع التوصيات والاقتراحات وتقديم الدراسات الخاصة بالتنمية والتعاون في مجال تكنولوجيا المعلومات والاتصالات.

ب- المساهمة في تنفيذ الأهداف التي يحددها "المجلس الوزاري" من خلال التفاعل بين الأطراف الرئيسية المشاركة فيه.

٥- الترحيب بدعوى دولة الإمارات العربية المتحدة لاستضافة الاجتماع الأول للمنتدي العربي لتكنولوجيا المعلومات والاتصالات.



٦- توجيه الأطراف المؤثرة في قطاع الاتصالات إلى العمل على إيجاد تعرفة معقولة ومتوازنة لخدمات الاتصالات بين الدول العربية، تضمن استمرار وتحديث مرافق الخدمة، وتدعم التنمية الاقتصادية والاجتماعية من خلال تيسير أسعار الخدمة التي يتحملها المستثمرون ورجال الأعمال والمواطنون في المنطقة العربية.

٧- وضع خطة لإقامة وتطوير شبكات الاتصالات وشبكات المعلومات العربية وتطوير نظم المعلومات المستخدمة على المستوى الحكومي والأجهزة الإدارية في الدول العربية والعمل على احتضان عدد من المؤسسات البحثية في الدول العربية لمدة زمنية محددة حتى تصل إلى العالمية في مستواها.

٨- دعوى صناديق التنمية ومؤسسات التمويل العربية لدعم جهود تطوير قطاع تكنولوجيا المعلومات والاتصالات على النطاق العربي، ودعوة الدول الأعضاء، من خلال ممثلها في صناديق التمويل ومؤسسات التنمية العربية إلى اتخاذ الإجراءات اللازمة لتوجيه نسبة متزايدة من مواردها لمشروعات التعاون العربي في هذا القطاع.

تكليف الأمانة العامة والمجلس الاقتصادي والاجتماعي بالتعاون مع مجلس وزراء الاتصالات العرب بمتابعة تنفيذ هذا القرار، ويقدم الأمين العام تقريراً إلى القمة العربية القادم عام ٢٠٠٢ حول ما يتم إنجازه من قبل المجلسين لتنسيق وتكثيف التعاون العربي في مجال الاتصالات وتكنولوجيا المعلومات بما في ذلك اقتراح الأنظمة القانونية اللازمة.

٩- الترحيب باحتضان تونس للقمة العالمية حول مجتمع المعلومات في عام ٢٠٠٣، والتي ينظمها الاتحاد الدولي للاتصالات والتأكيد على أهمية هذا الملحق الدولي الذي من شأنه أن يعزز الدور العربي في

النهضة المعلوماتية في العالم. ودعوى الدول الأعضاء لحضور هذا  
الملتقى للمساهمة في إثرائه ودعمه ماديا باعتبار انعكاساته الإيجابية  
على تطوير تكنولوجيا المعلومات في العالم العربي<sup>(١)</sup>.

أصدر مجلس جامعة الدول العربية علي مستوى القمة (١٦) المنعقد  
بستونس يومي ٢٢-٢٣ مايو/ أيار ٢٠٠٤ قراراتين بشأن مجال الاتصالات  
والمعلومات ، كما تضمن بيانه الختامي فقرات حوله، وفيما يلي نص  
القرارين وفقرات البيان ذات العلاقة:

#### أولاً: القرارات:

أ- قرار مجلس الجامعة علي مستوى القمة بشأن القمة العالمية لمجتمع  
المعلومات<sup>(٢)</sup>.

١- التأكيد علي أهمية المشاركة العربية علي أعلى المستويات في القمة  
التي ستعقد في تونس سنة ٢٠٠٥ وكذلك علي أهمية المرحلة الثانية  
من القمة العالمية لمجتمع والطابع العملي التتموي الذي تكتسبه.

٢- التأكيد علي أهمية مواصلة التنسيق العربي والإعداد الجيد  
والمشاركة المكثفة الفعالة في التحضير للمرحلة الثانية للقمة التي  
ستعقد في تونس من ١٦ إلى ١٨ نوفمبر / تشرين ثاني ٢٠٠٥.

٣- التأكيد على أهمية تفعيل الاستراتيجية العربية المعتمدة في مجال  
الاتصالات والتقنية المعلوماتية وضرورة إعداد خطة عمل عربية  
لاعتمادها في نطاق المرحلة الثانية للقمة.

٤- دعوة المنظمات ذات الصلة للمساهمة الفعالة في إنجاح مختلف  
المواعيد التي تدرج في إطار الإعداد للقمة.

(١) (ق.ق: ٢١٤ د.ع- ٢٨/٣/٢٠٠١).

(٢) المرحلة الثانية- تونس ٢٠٠٥.

٥- تكليف مجلس الوزراء العرب للاتصالات والمعلومات بمواصلة التحضير العربي الجيد للمرحلة الثانية للقمة العالمية لمجتمع المعلومات المقرر انعقادها بالجمهورية التونسية خلال الفترة من ١٦ - ١٨ نوفمبر / تشرين ثاني ٢٠٠٥.

٦- التأكيد أن عملية تطوير تكنولوجيا الإعلام والاتصال واستيعاب مجمل تقنياتها وتطبيقاتها الرقمية بين دول العالم من الأدوات الرئيسية الهادفة إلى إرساء مجتمع متكافئ ومتوازن وتحقيق للتنمية الشاملة. قرر مجلس الجامعة على مستوى القمة بشأن المنظمة العربية لتكنولوجيا الاتصالات والمعلومات.

- الطلب من الدول الأعضاء استكمال المصادقة على النظام الأساسي للمنظمة العربية لتكنولوجيا الاتصالات والمعلومات، حتى يتم الإعلان عن تأسيسها وبدء ممارسة نشاطها، قبل المرحلة الثانية للقمة العالمية لمجتمع المعلومات.

ثانيا: البيان الختامي<sup>(١)</sup>

بشأن رآب الفجوة الرقمية بين الدول العربية وغيرها من الدول:

٣٨- يؤكد القادة على أهمية بلورة وإقامة مشروعات عربية محددة في مجالات البنية الأساسية للاتصالات والمعلومات والتنمية البشرية والبيئة المعلوماتية والتجارة الإلكترونية.

بشأن القمة العالمية لمجتمع المعلومات:

٣٩- يؤكد القادة على أهمية مواصلة التحضير العربي للمرحلة الثانية للقمة المقرر انعقادها في الجمهورية التونسية في ١٦ - ١٨ نوفمبر / تشرين الثاني ٢٠٠٥، وعلى المشاركة العربية على أعلى المستويات في هذه القمة.

(١) الفقرات ٣٨، ٣٩، ٤٠

٤٠- بشأن المصادقة على النظام الأساسي للمنظمة العربية لتكنولوجيا الاتصال والمعلومات.

يؤكد القادة على أهمية الإسراع في استكمال إجراءات المصادقة على النظام الأساسي للمنظمة العربية لتكنولوجيا الاتصال والمعلومات وبدء ممارسة نشاطها قبل المرحلة الثانية للقمة العالمية لمجتمع المعلومات<sup>(١)</sup>. وقد انتهت القمة العربية من أعمالها قبيل صدور جدول الأعمال مباشرة، والنتائج معروضة للتفضل بالإحاطة واتخاذ ما يلزم.

---

(١) تونس ٢٠٠٥.

**ثامنا**

**وثيقة إعلان الاستراتيجية العربية  
لمجتمع الاتصالات وتقنية المعلومات**



## وثيقة إعلان

### الاستراتيجية العربية لاجتماع الاتصالات

#### وتقنية المعلوماتية

أولاً: الفجوة التكنولوجية والعلمية والاقتصادية بين الدول العربية وبعض البلدان التي لها نفس البدايات التنموية:

أصبح من الثابت أن شكل العالم اليوم وغدا هو نتاج العلم والتكنولوجيا خلال المائة سنة الأخيرة. فالعالم اليوم يتم تقسيمه إلى دول غنية اقتصادياً لها قوة وتملك القدرة على التحكم في مواردها من خلال إنتاج وإتقان واستخدام العلم والتكنولوجيا وهي في الغالب دول الشمال... ودول أخرى فقيرة اقتصادياً لها ضعيفة ويتحكم في مواردها عوامل خارجية بسبب قصور في الطاقات العلمية والتقنية وعدم تمكنها من إنتاج وإتقان واستخدام العلم والتقنية في الأنشطة الإنتاجية والاقتصادية المختلفة وهي في أغلب الأمر دول الجنوب.

والواقع يشير إلى أن الفجوة في الاقتصاد بين الشمال والجنوب هي في المقام الأول فجوة في علوم وتقنية الاتصالات والمعلومات. وفي هذا الصدد يشير تقرير لمنطقة اليونسكو صادر في عام ١٩٩٣ عن حالة العلم في العالم إلى أن البداية الذهبية للانضمام لقافلة النور الاقتصادية الآسيوية والأفريقية هو من خلال بوابة وتقنية المعلوماتية والبحث العلمي. وفي نفس الاتجاه قد أشارت الكثير من الأعلام العربية إلى أن السبيل الوحيد لأن تتحول دول المنطقة العربية إلى نمو حقيقي يتوازن ويتنافس مع النور الآسيوية وغيرها من الدول النامية هو تنمية وتطوير كل من آليات البحث العلمي والصناعات التقنية المتقدمة خاصة تلك المتعلقة بتقنية الاتصالات والمعلوماتية. بل ذهب البعض إلى التأكيد على أن الفجوة الاقتصادية - إذا ما استثنينا العائدات البترولية لبعض الدول العربية - بين هذه الدول وبعض البلدان التي لها نفس

البدايات التتموية مثل كوريا الجنوبية، إندونيسيا، وماليزيا وغيرها إنما مردها في المقام الأول إلى الفجوة في استخدام وإنتاج وسائل تقنية الاتصال والمعلوماتية التي تطورت تطورا عظيما خلال السنوات الخمس والعشرين الأخيرة. وتظهر هذه عند عقد مقارنات لمؤشرات اقتصادية رئيسية هامة مثل الدخل القومي للفرد وإنتاجية العامل والقيمة المضافة لعمله وفي قيمة التصدير (عدا البترول).

ومع بداية القرن الواحد والعشرين وما ينتظر فيه من ثورة تقنية عارمة بدأت مظاهرها الآن في التقنيات الحديثة خاصة تلك المتعلقة بالاتصالات والمعلوماتية وما يصاحبها من شفافية معلوماتية ووصولاً إلى مجتمع الاتصالات والمعلوماتية الشامل أصبحت بداية انطلاقة مجتمع الاتصالات والمعلوماتية العربي الآن أمرا محتوما إذا قدر للأمة العربية أن تسود في مجتمع دولي أصبحت السيادة فيه لمن يمتلك تقنية والمعلوماتية والتبعية للآخرين.

ولإظهار سعة الفجوة التي يجب على الأمة العربية اجتيازها نجد أنه إذا كان إنتاج العالم عام ٢٠٠٠ من صناعات التقنية والمعلوماتية يصل إلى نحو ١,٢ ترليون دولار (١,٢٠٠ مليار دولار) وإذا كان عدد سكان الدول العربية يمثل نحو ٤% من عدد سكان العالم فإن نصيب المنطقة العربية من هذه المنتجات عام ٢٠٠٠ يجب أن يكون على الأقل ٤٨ مليار دولار بينما هو لا يتعدى الآن نسبة ضئيلة من هذا الرقم.

إن عواقب عدم إعلان الإنطلاقة التقنية والمعلوماتية العربية الآن وخيمة لا يمكن تخيلها إذ أنها ببساطة تعني أن الأمة العربية لن تتواجد كعضو عامل في نادر التحضر للقرن الجديد وما بعده. فعلى الصعيد الاقتصادي نجد أن النظام الدولي الجديد ممثلا في منطقة التجارة العالمية واتفاقيات الجات وغيرها يزيد من القوة النسبية للقوى ويزيد من الضعف النسبي للضعيف مما يحول الفجوة التقنية والمعلوماتية إلى فجوة اقتصادية لها أثر المدمر على أمن المنطقة.



ومن ناحية أخرى لابد من التأكيد على أهمية تجاوز الفجوة العلمية- البحثية كشرط أساسي لابد منه لاقتحام القرن الحادي والعشرين، وذلك بسبب انخفاض مستوى التعليم وانتشار الأمية التي تصل إلى ٤٠% في المتوسط بين الرجال و ٧٠% في المتوسط بين النساء وكذلك انخفاض مستوى الخلق والإبداع في مجال البحث العلمي والتقني، ذلك أن معدل الاستثمار في هذا الجانب أنسي من ١% سنوياً من الناتج القومي، في حين تتعارف باقي حكومات بلدان العالم ومؤسساتها الخاصة على تخصيص ما لا يقل عن ٣% من دخلها للاستثمار في مجال البحث والتطوير، لذلك ليس من المستغرب أن تكون حصة للبلدان العربية من الاكتشافات العلمية المسجلة عليه دولياً المستوى العربي "ضئيلة جداً" إن لم تكن معدومة.

ومن المهم جداً التركيز على هذا الجانب حيث نقيم بلدان العالم اليوم كقوة سياسية واقتصادية يجري على أساس مساهمته في الاكتشافات العلمية المسجلة دولياً<sup>(١)</sup>.

أن أهم مبرر على الإطلاق لتبني الاستراتيجية العربية لتقنية المعلومات ليس مدى الربح الذي سنجنيه من تطبيقها، وهو بلا شك كبير، بل يكمن في التأكيد على أن المبرر الأكبر هو تقدير مدى الخسارة التي ستلحق بنا فيما لو لم ننفذ هذه الاستراتيجية. أن العرب اليوم مجبرون على تبني استراتيجية عربية لتكنولوجيا المعلومات، ويبدو التساؤل اليوم عن جدوى تبنيها أشبه بالتساؤل عن جدوى استخدام المطبعة بدلاً من نسخ المخطوطات في المجتمع القديم، لذلك يجب أن نعني أن التحولات النوعية التي تطرأ على تطوير المجتمع هي ممرات إجبارية لا يمكن طرحها بصيغة التساؤل عن جدوى

(١) (حيث تساهم الولايات المتحدة بأكثر من ٥٥% من هذه الاكتشافات تليها اليابان بنسبة ١٨ % ثم الاتحاد الأوروبي ١٥% وبقي دول العالم بنسبة ١٢%).

عبورها، بل يجب أن يكون التساؤل عن كيفية العبور لضمان تنفيذه بأيسر السبل وأقصرها وأقلها وأعلاها مردودا.

وتقدم الاستراتيجية العربية لتقنية المعلومات دعما كبيرا للتعاون العربي، لأنها تهيئ لانطلاق مشاريع اقتصادية كبيرة يمكن أن تطلق كنتيجة لنجاح تلك الاستراتيجية العربية، إذ أن تنفيذ هذه الاستراتيجية يخلق قنوات عصرية لتبادل المعلومات بين صناعات القرار العربي في المجالين السياسي والاقتصادي وعلى جميع مستويات سلم الإدارة وصنع القرار، مما يشكل أول خطوة فعلية لتبادل المعلومات بصورة منتظمة ويسهل انتقال التعاون العربي في المجالات الصناعية والتجارية والزراعية وإلى دعم البحث التطبيقي المشترك.

وتعمل كثير من المؤسسات الرسمية والشركات الخاصة في أوروبا على جمع وتنظيم المعلومات العلمية ونقل المعرفة، وعرض هذه المعلومات المنظمة والمحفوظة على أفراس ليزرية كبسولة رائجة في الاقتصاد، وأن البلدان العربية بما لها من امتداد يؤمن سوقا واسعة تتضمن الأسواق العربية أي أسواق أكثر من عشرين دولة تستطيع الإفادة من هذا النوع من الصناعات، بل ربما كان هذا النوع من صناعة المعلومات هو الأنسب لهذه المرحلة، حيث أنه يؤمن تشغيل جميع الفعاليات العاملة في مجال تكنولوجيا المعلومات ويؤسس لقاعدة متينة تدعم التطور العلمي والبحث والقدرة على الإبداع والابتكار في البلدان العربية، ومن ناحية أخرى فإن هذا المجال الذي تزداد الحاجة إليه اليوم هو القادر بما يحققه من نجاح على تحقيق التمويل اللاحق لمشروعات أكبر في المستقبل.

**ثانيا: الصناعات المعتمدة على تقنيات الاتصالات والمعلوماتية:**

على الرغم من الأهمية المتنامية للصناعات المعتمدة على تقنيات الاتصالات والمعلوماتية المتقدمة على مستوى العالم ككل، إلا أنه لا يوجد

تعريف واضح ومقبول بشكل عام لها. ومن المتفق عليه أن هذه الصناعات هي تلك التي يعتبر فيها الفكر أو الجهد البشري الخلاق Knowledge المصدر الرئيسي للمزايا التنافسية للمنتخبين، وكننتيجة لذلك فعادة ما يضطلع هؤلاء باستثمارات ضخمة في مجال خلق وتنمية ذلك الفكر والجهد البشري. وكانعكاس طبيعي لذلك المفهوم، فإنه عادة ما يتم التعرف علي الصناعات التكنولوجية المتقدمة بتلك التي تتطوي علي نسبة انفاق فوق المتوسط علي البحوث والتطبيقات والتطوير أو نسبة توظيف فوق المتوسط للعلماء والمهندسين، أو كليهما.

هذا ويمكن القول بأن الصناعات المعتمدة علي تقنيات الاتصالات والمعلومات هي الصناعات التقنية المتقدمة التي تضم المجالات الإنتاجية ذات القيمة المضافة العالية والتي تعتمد أساسا علي الفكر أي الجهد البشري الخلاق وهي تضم علي سبيل المثال:

- ١- الالكترونيات والاتصالات.
- ٢- تكنولوجيا المعلومات.
- ٣- الطاقة الجديدة والمتجددة.
- ٤- تكنولوجيا المواد الجديدة.
- ٥- الهندسة الوراثية والتكنولوجيا الحيوية.
- ٦- العدد وأدوات الإنتاج عالية التقنية.
- ٧- الأجهزة والمعدات الطبية.
- ٨- تكنولوجيا تصنيع الخامات الدوائية وكيمائياتها الوسيطة.
- ٩- تكنولوجيا الزراعة.
- ١٠- صناعة البحوث والتطوير.

١١- التصميم.

١٢- التكريب.

ولا شك في وجود عدد من الصناعات البينية التي تجمع بين مجالين أو أكثر مثل تكنولوجيا تنمية الصحراء بإدخالها في الدورة الاقتصادية للدولة حيث يمكن أن يشمل جميع المجالات المذكورة. وذلك بالإضافة إلى الصناعات المغذية والمكملة لهذه المجالات.

وحيث أن الصناعات المذكورة تمثل تكنولوجيات القرن الواحد والعشرين فإن هذا يظهر حتمية الاهتمام بتقنيات الاتصالات والمعلوماتية.

ثالثاً: انطلاقة مجتمع الاتصالات وتقنية المعلومات العربي:

أ- الهدف الاستراتيجي:

الهدف الاستراتيجي من تحقيق الانطلاقة هو تحويل المنطقة العربية إلى منطقة منتجة ومستخدمة ومصدرة للتقنية المتطورة للاتصالات والمعلومات للإسراع بالتنمية الاقتصادية والاجتماعية من خلال خلق قاعدة إنتاجية عريضة تعتمد في المقام الأول على القطاع الخاص تعمل في هذا المجال وتقوم بالتبعية بتطوير المجتمع بكامل مكوناته للوصول به إلى مجتمع يعتمد على تقنية الاتصالات والمعلوماتية متناغماً في ذلك مع الاتجاه المستقبلي للعالم المتقدم وذلك بحلول عام ٢٠٢٠.

ولا شك في أن الوصول إلى تحقيق هذا الهدف الاستراتيجي يستلزم وجود شراكة قوية بين جميع القوى المؤثرة في المجتمع العربي مثل الحكومات والإعلام والأجهزة التشريعية وقطاعات الأعمال الخاصة والعامة ومؤسسات التعليم والجمعيات غير الحكومية وغيرها على أن تكون القناعة المشتركة لها جميعاً هي أن تنمية صناعات التقنية والمعلوماتية يجب أن تكون المفتاح المستقبلي الأمل لاقترام القرن الواحد والعشرين.

## ب- المفاهيم الأساسية لمحاور الانطلاقة:

إن الدروس المستفادة من تجارب كافة الدول التي سبقتنا في هذا المجال- مثل النمر الأسيوية- تظهر أن الأسس التي يجب أن يقوم عليها البرنامج القومي لانطلاقة مجتمع التقنية والمعلوماتية تشمل المحاور التالية:

### المحور الأول: تهيئة المناخ العام وتشجيع الاستثمار:

لا شك في أن إعلان التأييد المطلق من القيادات السياسية لهذا البرنامج كأولوية قومية قصوى هو شرط وجوبي لإنجاحه حيث تقوم الحكومات بتوفير المناخ المغزى والدافع لنمو هذه الصناعات من خلال التشريعات والقوانين المحفزة للاستثمار وكذلك توفير البنية التحتية الملائمة بينها يتحمل القطاع الخاص في الأساس مهمة نقل المعرفة والتقنية وتشغيل العمالة والنفوض بالاقتصاد.

وكذلك فإن العبء الأكبر لنهضة هذه الصناعات بالعالم أجمع يقع علي عاتق شركات القطاع الخاص الصغيرة والمتوسطة مما يجعل الاهتمام بها ودعمها واجب أساسي للبرنامج وكذلك لكونها "رسل التقنية للمجتمع".

وحتى يمكن تحفيز رأس المال الخاص علي الاستثمار في هذه الصناعات رغم ما فيها من عنصر مخاطره في مصاريف البحث والتطوير والتحديث اللازمين لبقائها وتقدمها خاصة في مراحل نموها الأولى يجب خلق آليات ائتمانية جديدة تتواءم مع طبيعة الصناعات التقنية لاحتوائها علي بنية رأسمالية مرتفعة في المستوى الفكري والتقني وليس أساسا في الأصول المادية الملموسة.

ومن المفضل دائما أن تقوم حكومات البلدان العربية بالاستثمار نطاق واسع في مجال الاتصالات وأتمته الأعمال الحكومية وإعادة تنظيم مؤسسات الدول بصورة عصرية ويعد ذلك شرطا أساسيا لزيادة الطلب علي

تطبيقات تقنية المعلوماتية والاتصالات وبالتالي لتحفيز القطاع الخاص علي الاستثمار في الصناعات التقنية المتقدمة.

#### المحور الثاني: تهيئة البنية التحتية للاتصالات وتقنية المعلومات:

أن الإطار الذي يدعم الجهود المبذولة من الدول العربية كأساس لما تصل إليه من نتائج يتطلب مؤكدا الإعداد المسبق وتهيئة البنية التحتية اللازمة للاتصالات وتقنية المعلومات مع وضع آلية لاستمرار تدفق الاستثمارات العامة والخاصة لتحديث تلك البنية وخاصة شبكات الاتصالات وتخفيض تكلفة الاستخدام في نقل المعلومات، الأمر الذي يتطلب وضع خطط لرفع معدل انتشار الخطوط التليفونية مع التوسع في استخدام تقنيات الشبكة الذكية وتسهيلات الخدمات التليفونية وخاصة خدمات الهواتف الخلوية (المحمول) والهواتف عبر الأقمار الصناعية مع زيادة استخدامات خدمات شبكة الإنترنت والخدمات الإلكترونية الأخرى إضافة إلي إصلاح وإعادة هيكلة الإدارات البريدية العربية.

ونظرا لما تمثله البنية التحتية من أساس فإن الإسراع في تنفيذ شبكة Digital Backbone علي مستوى المنطقة العربية لتشمل أحدث التقنيات. وتحديث شبكة الربط الإقليمي العربي لضمان سهولة نقل البيانات والمعلومات يمثل أحد عوامل اللحاق بتلك الدول السابقة في هذا المضمار.

كذلك الاستثمار الجيد للترددات داخل الوطن العربي مع إجراء التنسيق اللازم مع المجتمع الدولي والتجمعات الإقليمية الأخرى.

ومن الضروري أن يكون التوجه العام خلال المرحلة القادمة في هذا الإطار من خلال تخصيص أراضي بالمناطق الصحراوية الجديدة وخارج المدن لإنشاء مناطق تجمع للصناعات التقنية والمعلوماتية تزود بالبنية التحتية المتكاملة والتي تشمل شبكة كابلات ضوئية واتصالات بالأمار الصناعية.

### المحور الثالث: تنمية الموارد البشرية:

الاستثمار في عقول الشباب العربي هو أهم ركيزة لتحقيق التقدم والانطلاقة التقنية ويشمل ذلك بما تمثله هذه القوة من طاقات منتجة ومستخدمة للتقنيات المتقدمة والمعلومات. ومن ثم فإن إعداد وتنفيذ خطط مكثفة وعاجلة للتنمية البشرية في التعليم والتأهيل والتدريب علي التقنيات المتقدمة يعد أساسا لا غني عنه لإنجاح البرنامج.

إن إعادة النظر في المناهج الدراسية العربية علي مستوى التعليم الأساسي والمتوسط والعالي يعد شرطا ضروريا للنجاح في تنمية الموارد البشرية في عصرنا، فالتعليم هو بوابة مجتمع المعلوماتية لذلك يجب التركيز في المناهج التعليمية علي الرياضيات والتقنية ويجب إعادة النظر في المناهج بما يكفل اكتساب الطلبة ومهارات هامة جدا وضرورية لعملهم المستقبلي وبشكل خاص: القدرة علي المحاكمة، البحث عن المعلومات وتجميعها وتنظيمها واستخلاص نتائج منها والتعامل مع تقنية المعلوماتية ومع مصادر المعلومات ومع التجارة الإلكترونية واقتصاد المعرفة، وعموما لابد من السعي إلي تطوير المعاهد المتوسطة والجامعات بما يناسب تزويد سوق العمل بالمهارات التقنية والعلمية المتقدمة، ولابد من الأکید علي أهمية التدريب الذاتي والتعليم المستمر وإقامة نقاط للتدريب الدائم في جميع المؤسسات الخاصة والعامة والحكومية.

كذلك فإن استمرارية الانطلاقة التقنية يستلزم الاهتمام الخاص بتأهيل الأطفال - من ٦ إلى ١٥ سنة - وإعدادهم إعدادا جيدا للتعامل مع أدوات عصر تكنولوجيا الاتصالات والمعلومات مما يمثل ولا شك أهم استثمار في مستقبل الأمة العربية.

ويجب أيضا الاهتمام بالتدريب المتخصص المكثف في مجالات حديثة لشباب الخريجين لتأهيل أجيال شابة من رجال الصناعة والأعمال وخاصة في مجالات إدارة المشروعات التقنية وفنون التسويق.

وكذلك ينبغي الاستفادة من الخبرات العربية العاملة في الخارج في مجالات التقنية والمعلومات وجذبها للمشاركة الفعالة في هذا البرنامج القومي.

**المحور الرابع: توسيع قاعدة قطاع أعمال تكنولوجيا الاتصالات والمعلومات:**

ويقع عبء تنفيذ هذا المحور أساسا علي عاتق القطاع الخاص إذ أن نجاح الانطلاقة يمكن قياسه بعدد الشركات الجديدة المنشأة وحجم إنتاج هذه الشركات ومدى جودة منتجاتها وقدرتها التنافسية في الأسواق العالمية وكذلك حجم العمالة الجديدة التي توفرها هذه الشركات.

وإنشاء الشركات الجديدة لا يجب أن يقتصر علي الشركات الصغيرة والمتوسطة ولكن يجب إنشاء شركات قطاع خاص عملاقة مثل شركة لإدارة مناطق الصناعات التقنية أو شركة لتسويق البرمجيات العربية وخدمات شركات البرمجة بغرض التصدير وكذلك شركة للتسويق الخارجي للمنتجات التقنية الأخرى.

وهنا لابد من التأكيد علي أهمية الدور الحكومي لدعم لتوسيع قطاع تقنية المعلوماتية والاتصالات وذلك من خلال تقديم دعم وتسهيلات مباشرة للاستثمارات الصغيرة والمتوسطة ومن خلال الدخول في الميدان كشريك مع القطاع الخاص في إنشاء شركات عملاقة متخصصة بتقنية المعلوماتية والاتصالات.

وحتى يمكن نقل واستيعاب التقنيات الحديثة والمتطورة وكذلك تطبيق قواعد الجودة العالمية في الأداء فيجب علي القطاع الخاص تشجيع الاستثمارات الأجنبية بمد الجسور مع الشركات الأجنبية ذات السمعة الطيبة



في مجالها وتنشيط التعاون معها. إذ أن التحالفات العالمية سواء مع دول بعينها أو مع شركات عملاقة يمثل أحد الوسائل المقبولة والمسلم بها لتوطيد التقنية ولاندماج التقني مع بقية العالم ويجب الاستفادة بالعلاقات العربية المتميزة مع بعض الدول المتقدمة لتحقيق ذلك الأمر الذي يتطلب مشاركة بعض المتخصصين لتوفير المعرفة اللازمة للمفاوض العربي بأبعاد صناعات تكنولوجيا الاتصالات والمعلوماتية واحتياجاتها حتى يمكن إدراج الأنشطة التقنية ضمن الاتفاقيات الثنائية والمتعددة مع الدول المتقدمة.

#### المحور الخامس: تنمية السوق المحلي والتصدير:

لا شك في أن تنشيط سوق التصدير لمنتجات صناعات التقنيات والمعلوماتية يحتاج إلى قاعدة قوية تتمثل في وجود سوق محلي نشط لهذه المنتجات وهذا يجب الاعتراف بأن آليات السوق وحدها لا تكفي كهيئة ملائمة لتنشئة هذه الصناعة وتميئها ما لم يتم التأثير على هذه الآليات وتوجيهها بوعي وإدراك.

لذا فمن الدروس المستفادة من تجارب الدول التي سبقتنا في هذا المجال نجد أنه للحكومات دور أساسي لتبني مشاريع تقنية متطورة تقوم بتنشيط السوق الداخلي لهذه المنتجات شريطة أن تكون لها قيمة كبيرة في تحسين أداء مؤسسات الدولة علاوة على ما سيكون لهذه المشروعات من تأثير فعال في نشر الوعي التقني والمعلوماتي للمجتمع العربي ككل أي أن دخول الحكومات كموجه ومشتري للتقنيات المتطورة والمنتجة محليا أمر حتمي لبدء عملية إنعاش هذه الصناعات، ولعل من الأمثلة الواضحة على هذا أن تقوم الحكومة بتبني مشروعات للتعليم والصحة وتطوير الأداء الحكومي باستخدام تكنولوجيا الاتصالات والمعلومات.

أما تنشيط سوق التصدير الخارجي فيقع عبئه الأول على القطاع الخاص وذلك عن طريق تكوين شركات تسويق عملاقة والاشتراك في المعارض

والأسواق الدولية وعقد الصفقات نيابة عن الشركات المنتجة وغير ذلك من الأنشطة لفتح أسواق جديدة.

وقد يقتصر دور الحكومات هنا علي المساهمة في الأنشطة السابقة وتطوير أداء المكاتب التجارية بالخارج وتوجيهها نحو معاونة قطاع صناعات التقنية والمعلومات في فتح أسواق جديدة.

ولا شك في أن إيجاد صيغ وسياسات للتعاون وتضافر الجهود بين الدول العربية علي المحاور الأربع السابقة سوف تؤدي إلي إيجاد قوة خلاقة تنفع شعوب الأمة العربية إلي فتح تقنيات القرن الواحد والعشرين من أوسع أبوابها.

**المحور السادس: استخدام تقنية الاتصالات والمعلوماتية لدعم تطبيقات التنمية الاقتصادية والاجتماعية:**

تشكل الأرضية العلمية والتقنية العربية المشتركة منطلقا لتطبيق الاستراتيجية العربية للمعلوماتية وهذا لهذه الاستراتيجية في الوقت نفسه، فلا يخفي علي أحد أن التنافس الاقتصادي العالمي بين الأمم، إنما يقوم علي العلم والتقنية باعتبار هذين العنصرين هما الأساس لخلق القوة والحياة لاستمرار التفوق في الاقتصاد وتحقيق التنمية الشاملة.

ويشكل تنظيم المعلومات العلمية ونقلها إلي الشكل الرقمي، أحد أوجه الاستثمار الأمثل في مجال تقنية المعلوماتية، وفي هذا المجال ينبغي علي الحكومات العربية أن تتبنى مبادرات خاصة لدعم المؤسسات العاملة في مجال المعلومات العلمية، انطلاقا من ضرورة وجود بنية معلومات عربية تجعل البنية التحتية قابلة للاستثمار والتطوير وقابلة لتقديم نتائج مفيدة وحيوية للمجتمع والاقتصاد. وأن وجود اللغة العربية المشتركة بين جميع البلدان العربية سيسهل إطلاق مبادرات مشتركة بين جميع الدول العربية، أو بين عدد محدود منها علي الأقل لتحقيق استثمارات ناجحة في مجال بنية المعلومات، والتي تعتمد أساسا

علي الاستثمار في مجال التدريب وفي مجال تنظيم المعلومات العلمية وتسويقها كسلعة اقتصادية عصرية، تؤدي دوراً مزدوجاً في دعم تطوير المؤسسات العلمية العربي من جهة، وفي تحقيق دخل اقتصادي هام يستطيع تمويل مراحل لاحقة من المبادرات لاحتكام القرن الحادي والعشرين.

**المحور السابع: توسيع مجالات البحث التطبيقي والتطوير ونقل التقنية:**

من أهم عناصر الاستراتيجية العربية لتقنية المعلوماتية هو دعم حركة البحث التطبيقي ونقل التقنية إلى البلدان العربية، ولا يمكن لهذه الاستراتيجية أن تحقق النجاح دون تنشيط ودعم الإنتاج الفكري العربية مع تشجيع الابتكارية والأفكار الجديد والحاضنة التكنولوجية في إطار يدعم الأفكار الجديدة، وأن أي استراتيجية تستجيب لهذه المتطلبات ستبقى استراتيجية ناقصة ومفتقرة إلى مرتكزات حقيقية في أرض الواقع وإلى مصادر حيوية لتطورها اللاحق. وأن على البلدان العربية أن تمد نسبة يتفق عليها من الميزانيات الحكومية ومن الدخل المتحقق في القطاع الخاص بغرض دعم قطاع البحث التطبيقي والتطوير ونقل وتنمية التقنية.

**رابعاً: البرنامج المقترح لانطلاق مجتمع الاتصالات وتقنية المعلوماتية العربي:**

**المحور الأول: تهيئة المناخ العام وتشجيع الاستثمار:**

م	الإجراء	العائد
١	إعلان القيادات السياسية العربية عن بداية انطلاق مجتمع الاتصالات وتكنولوجيا المعلومات العربي للمجتمع العربي وللعالم أجمع.	- تعبئة المجتمعات العربية بكافة قوتها المؤثرة الحكومية وغير الحكومية. - إعطاء العالم الخارجي دليلاً على جدية الجهود العربية في هذا المجال.

م	الإجراء	العائد
٢	أن يكون مجلس وزراء الاتصالات العرب هو الهيئة التنفيذية العليا لتنمية مجتمع الاتصالات والمعلوماتية العربي. ويتخذ الإجراءات اللازمة لتحقيق ذلك من خلال مكتبة التنفيذي ولجانه التابعة له.	- وضع البرنامج القومي العربي لانطلاقه مجتمع الاتصالات والمعلومات حتى عام ٢٠٢٠ ومتابعة تنفيذ البرنامج وتطويره طبقاً للواقع. - وضع معوقات تنفيذ البرنامج دورياً أمام مجالي القمة العربية والمسئولين واقتراح الحلول لها ومتابعة تنفيذ هذه الحلول.
٣	حث الدول العربية علي إصدار قوانين جديدة وخدمات المعلوماتية لتنظيم مرافق الاتصالات وحماية الملكية الفكرية علي برامج الحاسب الآلي وغيرها من خلال آليات تتناسب معها لأوضاع تتميز بالشفافية وتقديم الخدمة الشاملة وحماية المستهلك وتحرير صناعة الاتصالات وفتح الأسواق المحلية للمنافسة الحرة لجميع خدمات الاتصالات وتشجيع الاستثمار في هذا المجال علي أسس غير	- تحرير صناعة المعلومات. - فتح الأسواق المحلية والعالمية للمنافسة الحرة.

م	الإجراء	العائد
	احتكارية وكذلك محاولة التنسيق بين هذه القوانين.	
٤	مراجعة التعريف الدولية لنقل المعلومات حتى تتناسب مع الأسعار العالمية مع مضاعفة سعة دوائر نقل المعلومات المتاحة حالياً داخليا وخارجيا وتخفيض تكلفة استخدامها وكذلك تخفيض التعريف التحاسبية والتحصيلية للخدمات الصوتية بين الدول العربية بحيث تكون أقل من مثيلتها مع الدول الأجنبية.	<ul style="list-style-type: none"> <li>- تشجيع شركات البرمجيات العالمية علي إنشاء فروع لها بالمنطقة العربية.</li> <li>- مساعدة شركات البرمجيات العربية علي الحصول علي تعاقدات من الشركات العالمية وخاصة في مجالات الحساب عن بعد وإدخال المعلومات وغيرها.</li> <li>- المساهمة في نشر التدريب والتعليم عن بعد باستخدام الحاسب الآلي والإنترنت.</li> </ul>
٥	تبادل الخبرات الفنية بين الإدارات العربية.	- زيادة الخبرة والتنسيق.
٦	التوجيه الإعلامي لدفع الوعي القومي بأهمية استخدام المنتجات التقنية.	- تعبئة الرأي العام في اتجاه التنمية التكنولوجية والمعلوماتية.
٧	إلغاء التعريف الجمركية والضرائب المباشرة وغير المباشرة علي انتقال برامج الحاسب ومنتجات تكنولوجيا المعلومات الأخرى بين الدول	- زيادة التعاون والتجارة في هذه المجالات بين الدول العربية.

م	الإجراء	العائد
	العربية.	
٨	إنشاء قاعدة بيانات متكاملة عن الكوادر البشرية المتاحة في المجالات المختلفة والمستوى التكنولوجي لهذه الكوادر	- تسهيل الاستعانة بهذه الكوادر في اختيار العاملين المدربين والمستشارين.

المحور الثاني: تهيئة البنية التحتية للاتصالات وتقنية المعلومات

م	الإجراء	العائد
١	الإسراع في تنفيذ شبكة Digital Backbone علي مستوى المنطقة العربية لتشمل أحدث التكنولوجيات وتحديث شبكة الربط الإقليمي العربي.	- سهولة نقل البيانات والمعلومات. - زيادة استخدام الإنترنت علي مستوى المنطقة العربية.
٢	وضع آلية لاستمرار تنفق الاستثمارات العامة والخاصة لتحديث البنية التحتية وخاصة شبكات الاتصالات وتخفيض تكلفة الاستخدام في نقل المعلومات.	- زيادة الاستثمار في مجالات الاتصالات والمعلومات.
٣	وضع خطوط لرفع معدل انتشار الخطوط التليفونية بالنسبة لعدد السكان مع التوسع في استخدام تقنيات الشبكة الذكية وتسهيلات الخدمات التليفونية مثل الرقم	- سهولة الاتصال. - زيادة استخدام خدمات شبكة الإنترنت والخدمات الإلكترونية الأخرى.

م	الإجراء	العائد
	المجاني والبريد الصوتي وبطاقات الاتصال المدفوعة مقنما والتوسع ونشر خدمة ISON وغيرها من الخدمات الحديثة وخاصة خدمات الهواتف الخلوية (المحمول) والهواتف عبر الأقمار الصناعية.	
٤	الاستثمار الجيد للترددات داخل الوطن العربي مع إجراء التنسيق اللازم مع المجتمع الدولي والتجمعات الإقليمية الأخرى.	- زيادة كفاءة استخدام الترددات.

المحور الثالث: تنمية الموارد البشرية

م	الإجراء	العائد
١	التوسع في تنفيذ البرنامج الإقليمي العربي لإعداد الطفل لدخول عصر التكنولوجيا والمعلومات من سن ٦ - ١٥ سنة (طفل القرن الواحد والعشرين) تساهم فيه المدارس والنوادي الاجتماعية ومكتبات الأطفال والجهات غير الحكومية.	- استثمار في مستقبل المنطقة العربية.
٢	وضع وتنفيذ برنامج إقليمي	- استثمار في مستقبل العرب.

م	الإجراء	العائد
	عربي لمحو الأمية الكمبيوترية والمعلومات لجميع طلاب المراحل الثانوية والجامعات خلال عشر سنوات ستكون بمثابة إضافة للمجهودات التي تقوم بها حاليا وزارات التعليم.	<ul style="list-style-type: none"> <li>- القيام بخطوة كبيرة نحو مجتمع التكنولوجيا والمعلومات.</li> <li>- إعداد المهارات الأساسية اللازمة للتدريب المتخصص في مجالات الصناعات التكنولوجية.</li> </ul>
٣	وضع وتنفيذ برنامج إقليمي عربي لتدريب وتأهيل الكوادر في مجالات الصناعات المعلوماتية المتقدمة.	<ul style="list-style-type: none"> <li>- تأهيل ١٥٠٠٠ مبرمج سنويا علي الأقل علي الأدوات الحديثة للبرمجة بمستوى عالمي.</li> <li>- تأهيل ٦٠٠ مصمم سنويا للدوائر الإلكترونية الدقيقة والتصميم والتصنيع باستخدام الحاسب الآلي بمستوى عالمي.</li> <li>- توفير الكوادر المتوسطة والعليا اللازمة للعمل بالشركات الجديدة في مجالات تكنولوجيا المعلومات المختلفة.</li> </ul>
٤	إنشاء جامعة أو أكاديمية عربية لتقنية الاتصالات والمعلوماتية وحث الدول العربية علي أحداث فروع في جامعاتها للاتصالات وتقنية المعلوماتية وتطوير مفاهيمها لتحقيق ورفع كفاءة الخريجين.	<ul style="list-style-type: none"> <li>- تخريج متخصصين ذوي مستوى متميز.</li> <li>- تدريب تخصصي لخريجي الجامعات والمعاهد العليا المختلفة.</li> <li>- توفير فرص متميزة للتعليم المستمر علي أحدث العلوم والتكنولوجيات باستخدام الإنترنت</li> </ul>



م	الاجزاء	العائد
		والتكنولوجيات الحديثة للتعلم والتعلم عن بعد. - تقديم خدمات بحثية متميزة. - المساهمة في التخطيط لتطوير تكنولوجيا عربية المنشأ- عالمية الأسواق.
٥	تطوير مناهج تكنولوجيا الاتصالات والمعلومات والرياضيات في الجامعات العربية وخاصة في كليات الحاسبات والهندسة والعلوم والتجارة وإعداد المعلم.	- رفع جودة الخريج في التخصصات ذات الصلة. - رفع كفاءة تدريس الحاسبات والتكنولوجيا في المدارس.
٦	إنشاء شبكة معلومات لربط الجامعات ومراكز البحوث العربية وكذلك شبكات للمعلومات المتخصصة (مثل شبكة المعلومات الصحية وشبكة المعلومات الجغرافية).	- تعاون في مجالات التعليم والتعليم عن بعد. - تعاون بحثي. - تعاون في تقديم خدمات متخصصة مثل التطبيق عن بعد والتخطيط العمراني.
٧	الاهتمام بالتعليم المستمر والتعليم عن بعد بواسطة الإنترنت لرفع كفاءة العاملين بالحكومة وقطاعات الأعمال.	- رفع كفاءة الأداء بالقطاع الحكومي وقطاعات الأعمال.

المحور الرابع: توسيع قاعدة قطاع الأعمال التكنولوجية والمعلوماتية:

م	الإجراء	العائد
١	دعم وتطوير حاضنات الصناعات والأنشطة التقنية والمعلوماتية وإنشاء شركة لضمان مخاطر الائتمان لهذه الصناعات والأنشطة.	- زيادة عدد الشركات. - زيادة العمالة. - زيادة التصدير
٢	المراجعة والتنسيق بين القوانين الخاصة بالتعاملات البنكية الإلكترونية مثل التوقيع الإلكتروني تشجيعا للتجارة الإلكترونية بين الدول العربية وبينها وبين الدول الأجنبية.	- زيادة تعاملات التجارة الإلكترونية.
٣	زيادة التعاون والتنسيق مع المجالس الوزارية والمنظمات الإقليمية المتخصصة المنبثقة عن الجامعة العربية مثل مجالس وزراء الإعلان والاتصالات والنقل والبيئة العرب ووسائل الإعلان الفضائية والمنظمات والاتحادات الأخرى ذات العلاقة بتقنية الاتصالات والمعلوماتية. كذلك زيادة التعاون والتنسيق	- زيادة الوعي. - زيادة التنسيق. - تشجيع العمل المشترك. - رفع جودة المنتج. - زيادة التصدير.

م	الإجراء	العائد
	مع المنظمات وصناديق التنمية الإقليمية والدولية ذات العلاقة وتشجيع إبرام اتفاقات تعاون ومنكرات تفاهم معها.	

المحور الخامس: تنمية السوق المحلي والتصدير:

م	الإجراء	العائد
١	طرح متطلبات الحكومة وقطاع الأعمال والقوات المسلحة من الأجهزة والتقنيات المتطورة لخطط التنمية القائمة علي قطاعات الصناعات التقنية والمعلوماتية الوطنية والإقليمية ومناقشة التقنيات الحديثة التي يمكن توفيرها محليا.	- دعم الشركات العاملة في المجال. - رفع جودة الإنتاج. - تنشيط السوق المحلي. - تحسين الأداء. - رشيد موازنة الجهات المختلفة نتيجة لانخفاض سعر المنتج المحلي.
٢	رصد موازنة من خلال الجهات المختصة للمساهمة في تسويق الأنشطة التكنولوجية والمعلوماتية خارجيا من خلال وسائل الإعلام والمعارض الدولية ووفود رجال الصناعة.	- زيادة التصدير.
٣	إعطاء الأولوية من قبل الشركات الوطنية والقومية	- زيادة كفاءة العملية التعليمية. - زيادة كفاءة الخدمات الصحية.

م	الإجراء	العائد
	المنتجة للبرمجيات بإنتاج حزم برامج جاهزة في المجالات القومية كالتعليم.	- تنمية السوق المحلي للبرمجيات. - زيادة سابقة أعمال الشركات الوطنية مما يساعدها في الحصول علي تعاقدات دولية.
٤	إنشاء هيئة تابعة للجامعة العربية لتنمية صادرات صناعات المعلومات العربية وكذلك إنشاء شركات عربية-عالمية لتسويق منتجات صناعة المعلومات العربية وتسويق إمكانات صناعة خدمات المعلومات عبر الإنترنت.	- زيادة فرصة التسويق الخارجي وداخل المنطقة العربية.
٥	إنشاء موقع علي الإنترنت لخصر أسواق البورصات العربية وتوفير المعلومات الأساسية عن صناعات المعلومات العربية والمؤشرات التنموية المتعارف عليها لكل دولة.	- توافر المعلومات الأساسية عن صناعات المعلومات العربية. - دعم اتخاذ القرارات وإرشاد المستثمرين والعملاء التجاريين. - المساعدة في إجراءات الدراسات والبحوث الاستراتيجية وغيرها في المجالات الاقتصادية والتنموية ذات الصلة.
٦	إنشاء شركة عربية للأعمال الإلكترونية مثل التجارة الإلكترونية والبريد الإلكتروني	- زيادة فرصة التصدير الخارجي وداخل المنطقة العربية.

م	الإجراء	العائد
	والمصارف الإلكترونية والتعليم عن بعد وغيرها.	
٧	إنشاء شركة عربية-عالمية لتصنيع مكونات الحاسب والأجزاء المكملة له والبرمجيات.	- زيادة فرصة التصدير الخارجي وداخل المنطقة العربية.

المحور السادس: استخدام تقنية الاتصالات والمعلوماتية لدعم تطبيقات التنمية الاقتصادية والاجتماعية:

م	الإجراء	العائد
١	وضع التشريعات المناسبة لضمان حقوق الملكية الفكرية وتأطير كافة الفعاليات والنشاطات ذات الصلة بالمعلومات وتقنياتها بقوانين تنظيم العمل في هذا المجال.	تشجيع القطاع الخاص ودعمه للاستثمار في مجال تكنولوجيا المعلومات والاتصالات وتنظيم المعلومات العلمية.
٢	العمل على تطوير بني المعلومات ودعم نظم المعلومات العصرية المتقدمة.	- خلق نشاط اقتصادي في مجال المعلومات وفي مجال للتدريب والبرمجة ودعم النشاطات العلمية والبحثية.
٣	وضع قاعدة بيانات WHO IS بأسماء المهنيين والاختصاصيين العرب في جميع المجالات العلمية.	- تسهيل إقامة مشروعات مشتركة بين البلدان العربية.

المحور السابع: توسيع مجالات البحث التطبيقي والتطوير ونقل التقنية:

م	الإجراء	العائد
١	توجيه المؤسسات الاقتصادية العربية الحكومية بتخصيص نسبة من دخلها للبحث التطبيقي والتطوير في مجال تخصصها.	- تأمين مصادر تمويل للبحث التطبيقي والتطوير ونقل التقنية.
٢	ربط البحث التطبيقي والتطوير بحاجات الاقتصاد والمجتمع من خلال تأسيس جهة تنسق بين مؤسسات البحث التطبيقي والتطوير العربية وبين الجهات المستفيدة من البحث التطبيقي والتطوير في القطاعين الحكومي والخاص.	- دعم تطوير البحث التطبيقي والتطوير ونقل التقنية وتمويله وتوجيهه باتجاه تلبية الحاجات الملحة للمؤسسات الاقتصادية.

## ثالثاً

١ - قانون الأونسيترال<sup>(١)</sup> النموذجي بشأن

التوقيعات الإلكترونية لعام ٢٠٠١

٢ - دليل اشتراء قانون الأونسيترال<sup>(٢)</sup>

النموذجي بشأن

التوقيعات الإلكترونية لعام ٢٠٠١

٣ - اتفاقية الأمم المتحدة المتعلقة باستخدام

الخطابات الإلكترونية

---

(١) لجنة الأمم المتحدة للقانون التجاري الدولي

(٢) لجنة الأمم المتحدة للقانون التجاري الدولي.

# ١ قانون الأونسيترال النموذجي بشأن التوقيعات

## الإلكترونية ٢٠٠١

### المادة ١: نطاق الانطباق

ينطبق هذا القانون حيثما تستخدم توقيعاً إلكترونياً في سياق أنشطة تجارية وهو لا يلغى أي قاعدة قانونية يكون القصد منها حماية المستهلكين.

### المادة ٢: التعاريف لأغراض هذا القانون

(أ) "توقيع إلكتروني" يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات.

(ب) "شهادة" تعني رسالة بيانات أو سجلاً آخر يؤكد أن الارتباط بين الموقع وبيانات إنشاء التوقيع.

(ج) "رسالة بيانات تعني معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل متشابهة، بما في ذلك، على سبيل المثال لا الحصر، التبادل الإلكتروني للبيانات أو البريد الإلكتروني أو البق أو التلكس أو النسخ البق.

(د) "موقع يعني شخصاً حائزاً على بيانات إنشاء توقيع ويتصرف إما بالأصالة عن نفسه وإما بالنيابة عن الشخص الذي يمثله.

(هـ) "مقدم خدمات تصديق" يعني شخصاً يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية.

(و) "طرف معول" يعني شخصاً يجوز أن يتصرف استناداً إلى شهادة أو إلى توقيع إلكتروني.



### **المادة ٣: المعاملة المتكافئة لتكنولوجيا التوقيع**

لا ينطبق أى من أحكام هذا القانون باستثناء المادة (٥) بما يشكل استبعاد أو تقييدا أو حرمانا من مفعول قانوني لأى طريقة لإنشاء توقيع إلكتروني تفى بالاشتراطات المشار إليها فى الفقرة ١ من المادة ٦، أو تفى على نحو آخر بمقتضيات القانون المطبق.

### **المادة ٤: التفسير**

١- يولى الاعتبار فى تفسير هذا القانون لمصدره الدولى وللحاجة إلى تشجيع توحيد تطبيقه ومراعاة حسن النية.

٢- المسائل المتعلقة بالأمر التى يحكمها هذا القانون ولا يسويها صراحة تسوى وفقا للمبادئ العامة التى يستند إليها هذا القانون.

### **المادة ٥: التغيير بالاتفاق**

يجوز الاتفاق على الخروج على أحكام هذا القانون أو تغيير مفعولها وما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير سارى المفعول بمقتضى القانون المنطبق.

### **المادة ٦: الامتثال لاشتراط التوقيع**

١- حيثما يشترط القانون وجود توقيع من شخص يعد ذلك الاشتراط مستوفى بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني موثوق به بالقدر المناسب للغرض الذى أنشئت أو أبلغت من أجله رسالة البيانات، فى ضوء كل الظروف بما فى ذلك أى اتفاق ذى صلة.

٢- تنطبق الفقرة ١ سواء أكان الاشتراط المشار إليه فيها فى شكل إلزام أم كان القانون يكتفى بالنص على تبعات تترتب على عدم وجود توقيع.

٣- يعتبر التوقيع الإلكتروني موثقاً به لغرض الوفاء بالالتزام المشار إليه في الفقرة ١ إذا:

(أ) كانت بيانات إنشاء التوقيع مرتبطة في السياق الذي تستخدم فيه بالموقع دون أي شخص آخر.

(ب) كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر.

(ج) كان أي تغيير في التوقيع الإلكتروني يجرى بعد حدوث التوقيع قابلاً للاكتشاف.

(د) كان الغرض من اشتراط التوقيع قانوناً هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجرى في تلك المعلومات بعد وقت التوقيع قابلاً للاكتشاف.

٤- لا تحد الفقرة ٣ من قدرة أي شخص:

(أ) على القيام بأي طريقة أخرى بإثبات موثوقية التوقيع الإلكتروني، لغرض الوفاء بالالتزام المشار إليه في الفقرة ١.

(ب) على تقديم دليل على عدم موثوقية التوقيع الإلكتروني.

٥- لا تنطبق أحكام هذه المادة على ما يلي:

#### المادة ٧: الوفاء بالمادة ٦

١- يجوز لـ (أي شخص أو جهاز أو سلطة تعينهم الدولة المشترعة جهة مختصة، سواء أكانت عامة أم خاصة) تحديد التوقيعات الإلكترونية التي تقي بأحكام المادة ٦ من هذا القانون.

٢- يتعين أن يكون أي تحديد يتم بمقتضى الفقرة ١ متسقاً مع المعايير الدولية المعترف بها

٣- ليس فى هذه المادة ما يخل بسريان مفعول قواعد القانون الدولى الخاص.

#### المادة ٨: سلوك الموقع

١- حيثما يمكن استخدام بيانات إنشاء التوقيع لإنشاء توقيع يكون له مفعوله القانوني، يتعين على كل موقع:

(أ) أن يمارس عناية معقولة لاجتناب استخدام بيانات إنشاء توقيعه إستخداما غير مأنون به.

(ب) أن يبادر، دون تأخر لا مسوغ له، إلى استخدام الوسائل التى يوفرها مقدم خدمات التصديق بمقتضى المادة ٩ من هذا القانون، أو على نحو آخر إلى بذل جهود معقولة لإشعار أى شخص يجوز للموقع أن يتوقع منه على وجه معقول أن يعول على التوقيع الإلكتروني أو أن يقدم خدمات تأييد للتوقيع الإلكتروني وذلك فى حالة:

١- معرفة الموقع بأن بيانات إنشاء التوقيع تعرضت لما يثير الشبهة.

٢- كون الظروف المعروفة لدى الموقع تؤدي إلى احتمال كبير بأن بيانات إنشاء التوقيع ربما تكون قد تعرضت لما يثير الشبهة.

(ج) أن يمارس ، فى حال استخدام شهادة لتأييد التوقيع الإلكتروني، عناية معقولة لضمان دقة واكتمال كل ما يقدمه الموقع من تأكيدات مادية ذات صلة بالشهادة طيلة دورة سريانها أو يتوخى إدراجها فى الشهادة.

٢- يتحمل الموقع للتبعات القانونية لتخلفه عن الوفاء باشتراطات الفقرة ١.

## المادة ٩: سلوك مقدم خدمات التصديق

١- حيثما يوفر مقدم خدمات التصديق خدمات لتأييد توقيع إلكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعاً، يتعين على مقدم خدمات التصديق المشار إليه:

(أ) أن يتصرف وفقاً للتأكدات التي يقدمها بخصوص سياساته وممارساته.

(ب) أن يمارس عناية معقولة لضمان دقة وإكتمال كل ما يقصده من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مدرجة في الشهادة.

(ج) أن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتمكن الطرف المعول من التأكد من الشهادة، مما يلي:

١- هوية مقدم خدمات التصديق.

٢- أن الموقع المعينة هويته في الشهادة كان يسيطر على بيانات إنشاء التوقيع في الوقت الذي أصدرت فيه الشهادة.

٣- أن بيانات إنشاء التوقيع كانت صحيحة في الوقت الذي أصدرت فيه الشهادة أو قبله.

(د) أن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتمكن الطرف المعول من التأكد عند الاقتضاء من الشهادة أو من سواها مما يلي:

١- الطريقة المستخدمة في تعيين هوية الموقع.

٢- وجود أي تقييد على الغرض أو القيمة التي يجوز أن تستخدم من أجلها بيانات إنشاء التوقيع أو أن تستخدم من أجلها الشهادة.

- ٣- أن بيانات إنشاء التوقيع صحيحة ولم تتعرض لما يثير الشبهة.
- ٤- وجود أى تقييد على نطاق أو مدى المسؤولية التى اشترطها مقدم خدمات التصديق.
- ٥- ما إذا كانت هناك وسائل متاحة للموقع لتقديم إشعار بمقتضى الفقرة ١ (ب) من المادة ٨ من هذا القانون.
- ٦- ما إذا كانت تتاح خدمة إلغاء آنية.
- (هـ) أن يوفر، حيثما تقدم الخدمات بمقتضى الفقرة الفرعية (د) "٥" وسيلة للموقع لتقديم إشعار بمقتضى الفقرة ١ (ب) من المادة ٨ من هذا القانون وأن يضمن حيثما تقدم الخدمات بمقتضى الفقرة الفرعية (د) "٦" إتاحة خدمة إلغاء آنية.
- (و) أن يستخدم فى أداء خدماته نظما وإجراءات وموارد بشرية جديرة بالثقة.
- ٢- يتحمل مقدم خدمات التصديق التبعات القانونية لتخلفه عن الوفاء بإشتراطات الفقرة ١.

#### **المادة ١٠: الجدارة بالثقة**

- لأغراض الفقرة ١ (و) من المادة ٩ من هذا القانون، يجوز لدى تقرير ما إذا كانت أى نظم وإجراءات وموارد بشرية يستخدمها مقدم خدمات التصديق جديرة بالثقة، أو مدى جدارتها بالثقة إيلاء الاعتبار للعوامل التالية:
- (أ) الموارد المالية والبشرية، بما فى ذلك توافر الموجودات.
- (ب) جودة نظم المعدات والبرمجيات.
- (ج) إجراءات تجهيز الشهادات وطلبات الحصول على الشهادات والاحتفاظ بالسجلات.

(د) إتاحة المعلومات للموقعين المعينة هويتهم فى الشهادات ولأطراف المعولة المحتملة.

(هـ) وجود إعلان من الدولة أو من هيئة اعتماد أو من مقدم خدمات التصديق بخصوص الامتثال لما سبق ذكره أو بخصوص وجوده.

(و) أى عامل آخر ذو صلة.

#### **المادة ١١: سلوك الطرف المعول**

يتحمل الطرف المعول التبعات القانونية الناجمة عن تخلفه عن:

- (أ) إتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني.
- (ب) إتخاذ خطوات معقولة، إذا كان التوقيع الإلكتروني مؤيدا بشهادة الأجل.
- ١- التحقق من صلاحية الشهادة أو وقفها أو إلغائها.
- ٢- مراعاة وجود أى تقييد بخصوص الشهادة.

#### **المادة ١٢: الاعتراف بالشهادات والتوقيعات الإلكترونية الأجنبية**

- ١- لدى تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني سارى المفعول قانونياً، أو مدى كونهما كذلك، لا يولى أى اعتبار لما يلي:
  - (أ) الموقع الجغرافي الذى تصدر فيه الشهادة أو ينشأ أو يستخدم فيه التوقيع الإلكتروني.
  - (ب) الموقع الجغرافي لمكان علم المصدر أو الموقع.
- ٢- يكون للشهادة التى تصدر خارج (الدولة المشرعة) المفعول القانوني نفسه فى (الدولة المشرعة) الذى للشهادة التى تصدر فى (الدولة المشرعة) إذا كانت تتيح مستوى مكافئاً جوهرياً من الموثوقية.
- ٣- يكون للتوقيع الإلكتروني الذى ينشأ أو يستخدم خارج (الدولة المشرعة) المفعول القانوني نفسه فى الدولة (الدولة المشرعة) الذى للتوقيع

الإلكترونى الذى ينسأه أو يستخدم فى الدولة (الدولة المشرعة) إذا كان يتتح مستوى مكافئاً جوهرياً من الموثوقية.

٤- لى تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني يتحان مستوى مكافئاً جوهرياً من الموثوقية لأغراض الفقرة ٢ أو الفقرة ٣ يولى الاعتبار للمعايير الدولية المعترف بها ولأي عوامل أخرى ذات صلة.

٥- إذا اتفقت الأطراف فيما بينهما، برغم ما ورد فى الفقرات ٢ و٣ و٤ على استخدام أنواع معينة من التوقيعات الإلكترونية أو الشهادات، يتعين الاعتراف بذلك الاتفاق باعتباره كافياً لأغراض الاعتراف عبر الحدود، ما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير سارى المفعول بمقتضى القانون المنطبق.

## ٢ دليل اشتراء قانون الأونسيترال النموذج بشأن

### التوقيعات الإلكترونية لعام ٢٠٠١

#### الصادر من لجنة الأمم المتحدة للقانون التجاري الدولي

##### الغرض من هذا الدليل

١- لدي إعداد واعتماد قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية (المشار إليه في ٨٥ ذا المنشور باسم "القانون النموذجي" أو القانون النموذجي الجديد)، كان في اعتبار لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال) أن القانون النموذجي سيكون أداة أكثر فاعلية لدى الدول التي تقوم بتحديث تشريعاتها، إذا قامت معلومات خلفية وتفسيرية إلى الفروع التنفيذية من الحكومات وإلى المشترعين، بغير مساعدة تلك الجهات علي استخدام القانون النموذجي. وكانت اللجنة مدركة أيضا لاحتمال استخدام القانون النموذجي في عدد من الدول التي لها إمام محدود بنوع تقنيات الاتصال الذي يتناوله القانون النموذجي. وهذا الدليل، الذي استمد جزء كبير منه من الأعمال التحضيرية للقانون النموذجي، يقصد به أيضا أن يكون مفيدا للجهات الأخرى التي تستخدم النص، مثل القضاة والمحكمين والاختصاصيين الممارسين والأكاديميين، وتلك المعلومات يمكن أيضا أن تساعد الدول لدى النظر في الأحكام التي ينبغي تعديلها، عند الاقتضاء، لكي تكون متوافقة مع أي ظروف وطنية معينة تستلزم ذلك التعديل. ولدي إعداد القانون النموذجي أيضا، افترض أنه سيكون مشفوعا بهذا الدليل. فمثلا تقرر، فيما يتعلق بعدد من المسائل، عدم تسويتها في القانون النموذجي، بل تناولها في الدليل، بغية توفير إرشاد للدول التي تشترع القانون النموذجي. ويقصد من المعلومات المقدمة في الدليل أن توضح السبب في إدراج أحكام القانون



النموذجي كعناصر أساسية جوهريّة في أداة قانونية ترمي إلى تحقيق أهداف القانون النموذجي.

٢- وقد أعدت الأمانة دليل الاشتراع هذا عملاً بطلب من الأونسيترال قدمته في ختام دورتها الرابعة والثلاثين، في عام ٢٠٠١ ويستند الدليل إلى مداولات ومقررات اللجنة في تلك الدورة<sup>(١)</sup>، التي اعتمدت فيها القانون النموذجي، وكذلك إلى آراء الفريق العامل المعني بالتجارة الإلكترونية، الذي اضطلع بالأعمال التحضيرية.

---

(١) الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17)، الفقرات ٢٠١-٢٨٤.



## الفصل الأول

### مقدمة للقانون النموذجي

أولاً: غرض القانون النموذجي ومنشأه:

أ- الغرض:

٣- بالنظر إلى تزايد استعمال تقنيات التوثيق الإلكترونية كبديل للتوقيعات الخطية وغيرها من إجراءات التوثيق التقليدية، نشأت فكرة الحاجة إلى إطار قانوني محدد يرمي إلى تقليل عدم اليقين بشأن المفعول القانوني الذي قد ينتج عن استخدام تلك التقنيات العصرية (التي يمكن أن يشار إليها عموماً بعبارة "التوقيعات الإلكترونية") فاحتمال اتباع نهج تشريعية متباينة في مختلف البلدان فيما يتعلق بالتوقيعات الإلكترونية يستدعي إيجاد أحكام تشريعية موحدة لإرساء القواعد الأساسية لتلك الظاهرة ذات الطبيعة الدولية أصلاً، حيث يكون الاتساق القانوني والصلاحيية التقنية للعمل بها تبادلياً (Interoperability) هدفاً مرغوباً في تحقيقه.

٤- بناءً على المبادئ الأساسية التي تستند إليها المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (والمشار إليه دائماً في هذا المنشور باسمه الكامل تجنباً للالتباس) فيما يتعلق بأداء وظيفة التوقيع في بيئة إلكترونية، يهدف هذا القانون النموذجي الجديد إلى مساعدة الدول على إقامة إطار تشريعي حديث ومنسق وعادل للتصدي بفعالية أكبر لمسائل التوقيعات الإلكترونية. ويقدم القانون النموذجي الجديد إضافة متواضعة - لكنها هامة - إلى قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، بتهيئة معايير عملية يمكن أن تقاس على أساسها قابلية التعويل التقنية على التوقيعات الإلكترونية، وعلاوة على ذلك يوفر القانون النموذجي صلة بين هذه قابلية التعويل التقنية والمفعول القانوني الذي يمكن انتظاره من توقيع إلكتروني

معين وبضيف القانون النموذجي إضافة كبيرة إلى قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، من خلال اعتماد نهج يمكن بموجبه تحديد المفهوم القانوني لأي تقنية توقيع إلكتروني معينة تحديدا مسبقا (أ) و تقييم صلاحيتها قبل أن تستخدم فعليا)، وعليه يقصد من القانون النموذجي أن يعزز فهم التوقيعات الإلكترونية، وأن يعزز الثقة بأن أي تقنيات توقيع إلكتروني معينة يمكن التعويل عليها في المعاملات العامة من الناحية القانونية، وفضلا عن ذلك، فالقانون النموذجي إذ يستحدث، مع الحرص على المرونة الواجبة، مجموعة من قواعد السلوك الأساسية لمختلف الأطراف التي يمكن أن تشترك في استخدام التوقيعات الإلكترونية (أي الموقعين والأطراف المعولة، والأطراف الثالثة التي تقدم خدمات التصديق)، فإنه يمكن أن يساعد على صوغ ممارسات تجارية أكثر تناسقا في البيئة الإلكترونية لوسائل التحكم والاتصالات.

٥- أما أهداف القانون النموذجي، التي تشمل التمكين من استخدام التوقيعات الإلكترونية أو تيسير استخدامها، وإتاحة معاملة متكافئة لمستعملي المستندات الورقية ومستعملي المعلومات الحاسوبية كذلك، فهي أهداف ضرورية لتعزيز عنصرَي الاقتصاد والكفاءة في التجارة الدولية وبإدراج الإجراءات المبينة في هذا القانون النموذجي (وكذلك أحكام قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية) في التشريع الوطني فيما يتعلق بالأحوال التي تختار فيها الأطراف استخدام وسائل الاتصال الإلكترونية، تنشئ الدولة المشتركة بطريقة مناسبة بيئة محايدة من حيث الوسائط، والمقصود بالنهج المحايد من حيث الوسائط، المستخدم أيضا في قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية هو النص من حيث المبدأ على استيعاب جميع الأحوال الواقعية التي تنشأ فيها المعلومات أو تخزين أو نقل، بصرف النظر عن الوسيلة التي قد تثبت عليها تلك المعلومات (انظر دليل تشريع قانون

الأونسيترال النموذجي بشأن التجارة الإلكترونية، الفقرة ٢٤)، وتعكس عبارة "بيئة محايدة من حيث الوسائط"، بالمعنى الذي استخدمت به قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، مبدأ عدم التمييز بين المعلومات التي تحملها وسيطة ورقية والمعلومات التي تبلغ أو تخزن إلكترونياً، وبالعكس القانون النموذجي الجديد، بنس القدر، مبدأ وجوب عدم التمييز بين التقنيات المتباينة التي يجوز أن تستخدم لتبليغ المعلومات أو تخزينها إلكترونياً، وهو مبدأ كثيراً ما يشار إليه بعبارة "الحيد إزاء التكنولوجيات" (انظر الوثيقة A/ CN. 9/484، الفقرة ٢٣).

ب- الخلفية:

٦- يشكل القانون النموذجي خطوة جديدة في سلسلة من الصكوك الدولية التي اعتمدتها الأونسيترال، والتي هي إما تركز تحديداً على احتياجات التجارة الإلكترونية وإما أعدت مع مراعاة احتياجات وسائل الاتصال الحديثة، وتشمل الفئة الأولى، أي الصكوك الموجهة تحديداً صوب التجارة الإلكترونية، على الدليل القانوني بشأن التحويلات الإلكترونية للأموال (١٩٨٧) وقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (١٩٩٦ و ١٩٩٨). وتشمل الفئة الثانية على جميع الاتفاقيات والصكوك التشريعية الدولية الأخرى التي اعتمدتها الأونسيترال منذ عام ١٩٧٨، والتي يعزز كلها الحد من الشكليات ويحتوي على تعاريف لعبارة "الكتابة" ي قصد بها أن تشمل رسائل الاتصالات التي ليس لها شكل مادي محسوس.

٧- أشهر صكوك الأونسيترال في ميدان التجارة الإلكترونية هو قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. وقد نتج إعداده في أوائل التسعينات عن تزايد استخدام وسائل الاتصال الحديثة مثل البريد الإلكتروني والتبادل الإلكتروني للبيانات لإجراء المعاملات التجارية الدولية. فقد أدرك أن التكنولوجيات الجديدة أخذت تتطور تطوراً سريعاً وستتطور بقدر أكبر من

اتساع نطاق إمكانية الوصول إلى وسائل تقنية داعمة مثل طرق المعلومات السريعة والإنترنت. غير أن بث المعلومات الهامة من الناحية القانونية في شكل رسائل غير ورقية، تعوقه عقبات قانونية تعترض استخدام تلك الرسائل، أو يعوقه عدم اليقين بشأن المفعول القانون لتلك الرسائل أو بشأن صحتها. وبهدف تيسير زيادة استعمال وسائل الاتصالات الحديثة، أعدت الأونسيترال قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. والغرض من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية هو أن يتيح للمشرعين الوطنيين مجموعة من القواعد المقبولة دولياً بشأن الكيفية التي تتيح إزالة عدد من هذه العقبات القانونية، والكيفية التي تتيح إنشاء بيئة قانونية أكثر أمناً لما أصبح يعرف باسم التجارة الإلكترونية.

٨- وقد اتخذ قرار الأونسيترال القاضي بصوغ تشريع نموذجي بشأن التجارة الإلكترونية نتيجة لكون التشريعات القائمة النازمة للاتصالات وتخزين المعلومات في عدد من البلدان غير واقية بالغرض أو غير مواكبة للتطور، لأنها لا تضع في اعتبارها استخدام التجارة الإلكترونية. وفي حالات معينة، لا تزال التشريعات القائمة تفرض قيوداً، أو تتطوي ضمناً على قيود، على استخدام وسائل الاتصال الحديثة وذلك مثلاً باشتراط استخدام مستندات "كتابية" أو "موقعة" أو "أصلية". وفيما يتعلق بمفاهيم المستندات "الكتابية" و "الموقعة" و "الأصلية"، اعتمد قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية نهجاً يستند إلى التناظر الوظيفي. ويستند نهج النظر الوظيفي إلى إجراء تحليل للأغراض والوظائف التي يؤديها الاشتراط التقليدي للمستندات الورقية، بهدف تحديد الكيفية التي يمكن بها أداء تلك الأغراض والوظائف من خلال تقنيات التجارة الإلكترونية (انظر دليل تشريع قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، الفقرات ١٥ - ١٨).

٩- وفي الوقت الذي كان يجري فيه إعداد قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، كان عدد قليل من البلدان قد اعتمد أحكاما محددة لمعالجة جوانب معينة من التجارة الإلكترونية، غير أنه لم يكن هناك تشريع يتناول التجارة الإلكترونية في مجملها، وهذا يمكن أن يؤدي إلى عدم اليقين بشأن الطابع القانوني للمعلومات التي تقدم في شكل غير المستند الورقي التقليدي وبشأن صلاحية تلك المعلومات. وعلاوة على ذلك، ففي حين أن القوانين والممارسات السليمة كانت ضرورية في جميع البلدان التي بدأ نطاق استخدام التبادل الإلكتروني للبيانات والبريد الإلكتروني يتسع فيها، كانت تلك الضرورة تلمس أيضا في بلدان عديدة فيما يتعلق بتقنيات اتصال مثل النسخ الرقمي والتكس. وبموجب المادة ٢ (ب) من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، يعرف التبادل الإلكتروني للبيانات بأنه نقل المعلومات إلكترونيا من حاسوب إلى حاسوب آخر باستخدام معيار متفق عليه لتمثيل المعلومات في بنية معينة.

١٠- كما ساعد قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية أيضا على معالجة مطالب ناشئة عن أن عدم كفاية التشريع على الصعيد الوطني تخلق عقبات أمام التجارة الدولية، إذ يرتبط قدر كبير منها باستخدام تقنيات الاتصال العصرية. ويلاحظ إلى حد كبير، أنه لا يزال من الممكن أن تسهم الفوارق بين النظم القانونية الوطنية التي تحكم استخدام تقنيات الاتصال المذكورة، وعدم اليقين بشأن تلك النظم، في الحد من مدى سبل وصول المنشآت التجارية إلى الأسواق الدولية.

١١- فضلا عن ذلك، فعلى الصعيد الدولي، يمكن أن يكون قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مفيدا في حالات معينة كوسيلة لتفسير الاتفاقيات أو الصكوك الدولية الأخرى القائمة التي تخلق عقبات قانونية أمام استخدام التجارة الإلكترونية، كأن تشترط، مثلا، تحرير مستندات معينة

أو شروط تعاقدية معينة في شكل كتابي. وفيما بين الدول الأطراف في تلك الصكوك الدولية، يمكن لاعتماد قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية كقاعدة للتفسير أن يهيئ وسيلة للاعتراف باستخدام التجارة الإلكترونية وأن يزيل الحاجة إلى التفاوض على بروتوكول ملحق بالصك الدولي المعني.

#### ج- الاستعراض التاريخي:

١٢- بعد اعتماد قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، قررت اللجنة، في دورتها التاسعة والعشرين في عام ١٩٩٦، أن تدرج في جدول أعمالها مسائل التوقيعات الرقمية وسلطات التصديق. وطلب إلى الفريق العامل المعني بالتجارة الإلكترونية أن يدرس مدى استصواب وجوى إعداد قواعد موحدة بشأن تلك المواضيع. واتفق على أن القواعد الموحدة التي ستعد ينبغي أن تتناول مسائل مثل: الأساس القانوني الذي ترتكز إليه عمليات التصديق، بما فيها التكنولوجيا الناشئة في مجال التوثيق والتصديق الرقمي، وإمكانية تطبيق عملية التصديق، وتوزيع المخاطر والمسؤوليات بين المستعملين ومقدمي الخدمات والأطراف الثالثة في سياق استخدام تقنيات التصديق، والمسائل المحددة المتعلقة بالتصديق عن طريق استخدام السجلات والإدراك بالإشارة<sup>(١)</sup>.

١٣- وكان معروضا على اللجنة في دورتها الثلاثين، في عام ١٩٩٧، تقرير الفريق العامل عن أعمال دورته الحادية والثلاثية (A/ CN. 9/437) التي أجريت بناء على منكرة أعنتها الأمانة (A/CN.9/WG.IV/WP.71). وقد بين الفريق العامل للجنة أنه توصل إلى توافق في الآراء حول أهمية وضرورة العمل على موازنة التشريعات في ذلك المجال. وفي حين أن الفريق العامل لم

(١) المرجع نفسه، الدورة الحادية والخمسون، الملحق رقم ١٧ (A/51/17)، الفقرات ٢٢٣ و ٢٢٤.



يُتخذ قراراً حاسماً حيال شكل ومضمون ذلك العمل، فقد خلص إلي استنتاجات أولية مؤداها أن من المجدي الاضطلاع بإعداد مشروع قواعد موحدة، علي الأقل بشأن مسائل التوقيعات الرقمية وسلطات التصديق، وبما بشأن مسائل التوقيعات الرقمية وسلطات التصديق، وبما بشأن المسائل ذات الصلة. وأشار الفريق العامل إلي أنه، إلي جانب التوقيعات الرقمية وسلطات التصديق، فإن الحاجة قد تدعو أيضاً أن تناول الأعمال المقبلة في مجال التجارة الإلكترونية ما يلي: مسائل البدائل التقنية للترميز بمفتاح عمومي، والمسائل العامة المتعلقة بالوظائف التي يؤديها مقدمو الخدمات من الأطراف الثالثة، والتعاقد الإلكتروني (A/ CN. 9/467، الفقرتان ١٥٦ و ١٥٧). وأقرت اللجنة الاستنتاجات التي توصل إليها الفريق العامل، وعهدت إليه بإعداد قواعد موحدة بشأن المسائل القانونية للتوقيعات الرقمية وسلطات التصديق.

١٤- أما فيما يتعلق بنطاق القواعد الموحدة وشكلها علي وجه الدقة، فقد اتفقت اللجنة عموماً علي أنه لا يمكن اتخاذ قرار ي هذه المرحلة من العملية، ورئي أنه، في حين أنه يمكن أن يكون من المناسب أن يركز الفريق العامل اهتمامه علي مسائل التوقيعات الرقمية، بالنظر إلي ما يؤديه الترميز بالمفتاح العمومي من دور بارز، فيما يبدو في ممارسات التجارة الإلكترونية الناشئة، فإن القواعد الموحدة ينبغي أن تكون متفقة مع النهج المحايد إزاء الوسائط السدي اتباع في قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. ولذا فإن القواعد الموحدة لا ينبغي أن تثبط العزيمة علي استخدام تقنيات تصديق أخرى. وعلاوة علي ذلك فقد يلزم، في تناول الترميز بالمفتاح العمومي، أن تراعي القواعد الموحدة مستويات مختلفة من الأمان وأن تعترف بالآثار القانونية المتباينة ومستويات المسؤولية المتباينة المرتبطة بالأنواع المختلفة من الخدمات التي تقدم في سياق التوقيعات الرقمية. وفيما يتعلق بسلطات التصديق، ففي حين أن اللجنة سلكت بقيمة المعايير التي تفرضها السوق،

رئيس علي نطاق واسع أنه قد يكون من المناسب أن يتوخي الفريق العامل استحداث مجموعة دنيا من المعايير التي ينبغي أن تقي بها سلطات التصديق، وخصوصا في حالة التماس التصديق عبر الحدود<sup>(١)</sup>.

١٥- وقد بدأ الفريق العامل في إعداد القواعد الموحدة (التي ستعتمد لاحقا باعتبارها القانون النموذجي) في دورته الثانية والثلاثين، استنادا إلي مذكرة أعتها الأمانة (A/CN.9/WG.IV/WP.73).

١٦- وكان معروضا علي اللجنة في دورتها الحادية والثلاثين، في عام ١٩٩٨، تقرير الفريق العامل عن أعمال دورته الثانية والثلاثين (A/CN.9/446)، ولوحظ أن الفريق العامل قد واجه، طيلة دورتيه الحادية والثلاثين والثانية والثلاثين، صعوبات جلية في التوصل إلي فهم مشترك للمسائل القانونية الجديدة الناشئة عن تزايد استخدام التوقيعات الرقمية وغيرها من التوقيعات الإلكترونية. ولوحظ أيضا أنه لم يتوصل بعد إلي توافق في الآراء بشأن الكيفية التي يمكن بها تناول تلك المسائل في إطار قانوني مقبول دوليا. غير أن اللجنة ارتأت عموما أن ما أحرز من تقدم حتى ذلك الحين يشير إلي أنه يجري صوغ القواعد الموحدة تدريجيا في هيكل صالح عمليا. وأعادت اللجنة تأكيد القرار الذي اتخذته في دورتها الثلاثين بشأن جدوى إعداد تلك القواعد الموحدة، وأعربت عن تقتها في إمكانية أن يحقق الفريق العامل مزيدا من التقدم في دورته الثالثة والثلاثين استنادا إلي المشروع المنقح الذي أعدته الأمانة (A/CN.9/WG.IV/WP.67) وفي سياق تلك المناقشة، نوهت اللجنة، مع الارتياح بأن الفريق العامل قد أصبح معترفا به عموما

(١) المرجع نفسه، الدورة الثانية والخمسون، الملحق رقم ١٧ (A/52/17)، الفقرات ٢٤٩-٢٥١.

باعتباره منتدى دوليا هاما بوجه خاص لتبادل الآراء بشأن المسائل القانونية للتجارة الإلكترونية ولإعداد حلول لتلك المسائل<sup>(١)</sup>.

١٧- ثم واصل الفريق العامل تنقيح القواعد الموحدة في دورتيه الثالثة والثلاثين، في عام ١٩٩٨، والرابعة والثلاثين، في عام ١٩٩٩، استنادا إلى مذكرات أعدتها الأمانة (A/CN.9/WG.IV/WP.76 و A/CN.9/WG.IV/WP.80) ويرد تقريرها الدورتين في الوثيقتين wp. و A/CN.9/457 و A/CN.9/454.

١٨- وكان معروضا على اللجنة في دورتها الثانية والثلاثين، في عام ١٩٩٩، تقرير الفريق العامل عن أعمال تينك الدورتين (A/CN.9/454 و A/CN.9/457). وأعربت اللجنة عن تقديرها للجهود التي بذلها الفريق العامل في إعداد القواعد الموحدة. وفي حين اتفق عموما على أن تقنما هاما أحرز في تينك الدورتين في فهم المسائل القانونية للتوقيعات الإلكترونية، رئي أيضا أن الفريق العامل واجهته صعوبات في التوصل إلى توافق في الآراء حول السياسة التشريعية التي ينبغي أن تستند إليها القواعد الموحدة.

١٩- وأبدي رأي مفاده أن النهج الذي يتبعه الفريق العامل حاليا لا يجسد بالقدر الكافي ما تحتاجه أوساط المنشآت التجارية من مرونة في استعمال التوقيعات الإلكترونية وغيرها من تقنيات التوثيق. فالقواعد الموحدة، كما كان يتوخاها الفريق العامل في ذلك الحين، كانت تركز تركيزا مفرطا على تقنيات التوقيع الرقمي وكذلك، في إطار التوقيعات الرقمية، على تطبيق محدد يتعلق بالتصديق من جانب طرف ثالث. واقتراح بناء على ذلك أن يكون عمل الفريق العامل فيما يتعلق بالتوقيعات الإلكترونية إما مقتصرًا على المسائل القانونية للتصديق عبر الحدود وإما أن يؤجل كلية إلى أن تصبح ممارسات

(١) المرجع نفسه، الدورة الثالثة والخمسون، الملحق رقم ١٧ (A/53/17)، الفقرات ٢٠٧-٢١١.

السوق أكثر رسوخا. وأبدي رأي ذو صلة مفاده أنه توخيا، لأغراض التجارة الدولية، ثم من قبل حل معظم المسائل القانونية الناشئة عن استخدام التوقيعات الإلكترونية، وذلك في قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (انظر الفقرة ٢٨ أدناه) مع أنه قد تكون ثمة حاجة، خارج نطاق القانون التجاري، إلى وضع لوائح تنظم استعمالات معينة للتوقيعات الإلكترونية، فإنه لا ينبغي للفريق العامل أن يشارك في أي نشاط تنظيمي من هذا القبيل.

٢٠- وكأن الرأي السائد على نطاق واسع أنه ينبغي للفريق العامل أن يواصل مهمته على أساس ولايته الأصلية وفيما يتعلق بالحاجة إلى قواعد موحدة بشأن التوقيعات الإلكترونية، أوضح بأن هيئات حكومية وتشريعية في بلدان كثيرة هي الآن بصدد إعداد تشريعات بشأن المسائل ذات الصلة بالتوقيعات الإلكترونية، بما في ذلك إنشاء مرافق المفاتيح العمومية (PKI) أو مشاريع أخرى تتعلق بمسائل وثيقة الصلة بذلك، وهي تنتظر تلقي الإرشاد من الأونسيترال في هذا الشأن (انظر الوثيقة A/ CN. 9/457، الفقرة ١٦). وفيما يتعلق بقرار الفريق العامل أن يركز على المسائل والمصطلحات الخاصة بمرافق المفاتيح العمومية، جري التنكير بأن تفاعل العلاقات بين ثلاث فئات متميزة من الأطراف (هي الموقعون وسلطات التصديق والأطراف المعولة) يناظر نمودجا محتملا واحدا لمرافق المفاتيح العمومية، ولكن يمكن تصور نماذج أخرى، ومنها مثلا عدم مشاركة أي مقدم خدمات تصديق مستقل. ورئي أن من الفوائد الرئيسية المتأتية من التركيز على المسائل المتعلقة بمرافق المفاتيح العمومية تيسير هيكلة القواعد الموحدة، وذلك بالإشارة إلى ثلاث وظائف (أو ثلاثة أدوار) فيما يتعلق بأزواج المفاتيح، وهي: وظيفة مدر المفتاح (أو صاحب المفتاح)، ووظيفة التصديق، ووظيفة التحويل. واتفق عموما على أن تلك الوظائف الثلاثة موجودة في

جميع مرافق المفاتيح العمومية واتفق أيضا علي ضرورة تناول تلك الوظائف الثلاث دور اعتبار لما إن كانت تؤديها في الواقع ثلاث هيئات منفصلة أو كان اثنتين منها الشخص نفسه (مثر كما في الحالة التي يكون فيها مقدم خدمات التصديق طرفا معولا أيضا). فضلا عن ذلك، رئي علي نطاق واسع أن التركيز علي الوظائف النمطية لمرافق المفاتيح العمومية، وليس علي أي نموذج أن يبسر في مرحلة لاحقة صوف قاعدة محايدة تماما من حيث الوسائط (انظر A/ CN. 9/457، الفقرة ٦٨).

٢١- وبعد مناقشة، أعادت اللجنة تأكيد قراراتها السابقة بشأن جدوى إعداد تلك القواعد الموحدة، وأعربت عن ثقتها في أن الفريق العامل يستطيع تحقيق المزيد من التقدم في دورته المقبلة<sup>(١)</sup>.

واصل الفريق العامل أعماله في دورتيه الخامسة والثلاثين، في أيلول/سبتمبر ١٠٠٠، والسادسة والثلاثين، في شباط/فبراير ٢٠٠٠، استنادا إلي مكرتئين أعدتهما الأمانة (A/CN.9/WG.IV/ WP.82 و A/CN.9/WG.IV/ WP.84). وكان معروضا علي اللجنة في دورتها الثالثة والثلاثين، في عام ٢٠٠٠، تقرير الفريق العامل عن أعمال تينك الدوريتين (A/CN.9/465 و A/CN.9/467). ولوحظ أن الفريق العامل اعتمد في دورته السادسة والثلاثين نص مشاريع المواد ١ و ٣ إلي ١٢ من القواعد الموحدة. وقيل أن بعض المسائل لا تزال بحاجة إلي التوضيح نتيجة لقرار الفريق العامل حذف مفهوم التوقيع الإلكتروني المعزز من القواعد الموحدة. وأعرب عن شغل مفاده أنه تبعا للقرارات التي سيتخذها الفريق العامل فيما يتعلق بمشروعي المادتين ٢ و ١٣، قد يلزم مراجعة بقية مشاريع الأحكام بغية اجتناب حدوث حالة يكون فيها المعيار الذي تضعه القواعد الموحدة مطبقا بنفس

(١) المرجع نفسه، الدورة الرابعة والخمسون، الملحق رقم ١٧ (A/54/17)، الفقرات ٣٠٨ - ٣١٤.

القدر على التوقيعات الإلكترونية التي تكفل مستوى عالياً من الأمان وعلى الشهادات المنخفضة القيمة التي قد تستخدم في سياق الرسائل الإلكترونية التي لا يكون مقصوداً منها أن تكون ذات مفعول قانوني هام.

وفي الدورة الثالثة والثلاثين، في عام ٢٠٠٠، أعربت اللجنة عن تقديرها للجهود التي بذلها الفريق العامل والتقدم الذي أحرزته في إعداد القواعد الموحدة، وحثت الفريق العامل على أن يكمل أعماله المتعلقة بالقواعد الموحدة في دورته السابعة والثلاثين<sup>(١)</sup>. ولدى إعداد القانون النموذجي، لاحظ الفريق العامل أنه قد يكون من المفيد تقديم معلومات إضافية بشأن القانون النموذجي تدرج في التعليق عليه. وعقب النهج المتبع في إعداد قانون الأونسيترال بشأن التجارة الإلكترونية، كان هناك تأييد عام لاقتراح بأن يكون القانون النموذجي الجديد مرفقاً بدليل يساعد الدول في تشريع القانون النموذجي وتطبيقه، والدليل. الذي يمكن أن يستمد كثير منه من الأعمال التحضيرية للقانون النموذجي. من شأنه أن يكون مفيداً أيضاً لمستعملي القانون النموذجي الآخرين. وقد طلبت اللجنة إلى الفريق العامل استعراض مشروع دليل الاشتراع الذي من المزمع أن تعدّه الأمانة.

٢٤- وقد أنجز الفريق العامل إعداد القواعد الموحدة في دورته السابعة والثلاثين، في أيلول/سبتمبر ٢٠٠٠، ويرد تقرير تلك الدورة في الوثيقة (A/CN.9/483. وفي سياق دورتيه السابعة والثلاثين والثامنة والثلاثين، ناقش الفريق العامل أيضاً مشروع دليل الاشتراع استناداً إلى مشروع أعدته الأمانة (A/CN.9/WG.IV/WP.88). ويرد تقرير الدورة الثامنة والثلاثين للفريق العامل في الوثيقة A/CN.9/484، الفقرة وطلب إلى الأمانة أن تعد صيغة منقحة لمشروع الدليل تتجسد فيها القرارات التي اتخذها الفريق العامل،

(١) المرجع نفسه، الدورة الخامسة والخمسون، الملحق رقم ١٧ (A/55/17)، الفقرات ٣٨٠-٣٨٣.

استنادا إلى مختلف الآراء والاقتراحات والشواغل التي كان قد أعرب عنها في تلك الدورة. وقد لاحظ الفريق العامل أن القواعد الموحدة (التي تتخذ شكل مشروع قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية)، إلى جانب مشروع دليل الاشتراع، سيقدمان إلى اللجنة لكي تستعرضهما وتعتمدهما في دورتهما الرابعة والثلاثين، في عام ٢٠٠١.

٢٥- وتحضير لدورة اللجنة الرابعة والثلاثين، جري تعميم نص مشروع القانون النموذجي، بصيغته التي وافق عليها الفريق العامل، على جميع الحكومات والمنظمات الدولية المهمة، وفي تلك الدورة، كان معروضا على اللجنة تقرير الفريق العامل عن أعمال دورته السابعة والثلاثين والثامنة والثلاثين، والتعليقات المتلقاه من الحكومات والمنظمات الدولية ( A/ CN. 9/492 و Add. 1- 3)، وكذلك مشروع دليل الاشتراع المنقح الذي أعدته الأمانة (A/ CN. 9/493) وعند بدء المناقشة، نظرت اللجنة في التعليقات المتلقاه من الحكومات والمنظمات الدولية (A/ CN. 9/492 و Add. 1- 3). وبعد أن استكملت اللجنة نظرها في المقترحات التي طرحتها الوفود بناء على التعليقات المقدمة من الحكومات والمنظمات الدولية المهمة، باشرت القيام باستعراض منهجي لمشاريع المواد وكذلك استعراض مشروع دليل الاشتراع الذي أعدته الأمانة (A/ CN. 9/493). ورهنا بما قد يكون ضروريا من التعديلات لتجسيد مداوات اللجنة ومقرراتها بخصوص نص القانون النموذجي ونص الدليل نفسه على حد سواء، وكذلك رهنا بأي تغييرات تحريرية قد تكون ضرورية لضمان الاتساق في المصطلحات، تبينت اللجنة أن نص مشروع الدليل يلبي على نحو واف بالعرض مقصد اللجنة في تقديم المساعدة إلى الدول التي تشترع القانون النموذجي الآخرين. وقد طلب إلى الأمانة إعداد صيغة نهائية من الدليل، ونشرها مع نص القانون النموذجي. وبعد أن نظرت اللجنة في نص مشروع القانون النموذجي بصيغته

التي نقحها فريق الصياغة، وفي مشروع دليل الاشتراع الذي أعدته الأمانة ( A/ CN. 9/493 )، اعتمدت المقرر التالي إبان جلستها ٧٢٧ المعقودة في ٥ تموز/ يولي ٢٠٠١.

- أن لجنة الأمم المتحدة للقانون التجاري الدولي.

- إذ تستذكر الولاية المسندة إليها بمقتضى قرار الجمعية العامة ٢٢٠٥ (د- ٢١) المؤرخ ١٧ كانون الأول/ ديسمبر ١٩٦٦، لأجل زيادة التنسيق والتوحيد والتدريجيين لقانون التجارة الدولية، مراعية في هذا الخصوص مصالح كل الشعوب ولا سيما شعوب البلدان النامية، في تطوير التجارة علي نطاق واسع.

- وإذ تلاحظ أن عددا متزايد من المعاملات في التجارة الدولية تتم بواسطة الاتصالات المتعارف عليها باسم "التجارة الإلكترونية" التي تشمل استخدام بدائل لأشكال الاتصال الورقية وخزن المعلومات وتوثيقها.

- وإذا تستذكر التوصية بشأن القيمة القانونية للسجلات الحاسوبية، التي اعتمدها اللجنة في دورتها الثامنة عشرة، المعقودة في سنة ١٩٨٥ وأن الفقرة ٥ (ب) من قرار الجمعية العامة ٤٠/ ٧١ المؤرخ ١١ كانون الأول/ ديسمبر ١٩٨٥، الذي طلبت فيه الجمعية إلي الحكومات والمنظمات الدولية أن تتخذ، حيثما اقتضى الأمر، إجراءات تتوافق مع توصية اللجنة من أجل ضمان الأمان القانوني في سياق استخدام التجهيز المؤتمت للبيانات في التجارة الدولية علي أوسع نطاق ممكن.

- وإذا تستذكر أيضا قانون الأونسيفرال النموذجي بشأن التجارة الإلكترونية يوفر مساعدة هامة للدول في إتاحة أو تيسير استخدام التجارة الإلكترونية من خلال تعزيز تشريعاتها التي تحكم استخدام بدائل أشكال



الاتصال الورقية وخزن المعلومات ومن خلال صوغ تشريعات حيث لا توجد حاليا.

- وإدراكا منها للفائدة الكبيرة من التكنولوجيات الجديدة المستخدمة لتبني هوية الأشخاص في التجارة الإلكترونية، والمتعارف عليها باسم "التوقيعات الإلكترونية".

- ورغبة منها في البناء على المبادئ الجوهرية التي تستند إليها المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية فيما يتعلق بأداء وظيفة التوقيع في بيئة إلكترونية.

واقترنا منها بأن اليقين القانوني في التجارة الإلكترونية سيزداد بتنسيق بعض القواعد المتعلقة بالاعتراف القانوني بالتوقيعات الإلكترونية على أساس محايد تكنولوجيا.

- واعتقادا منها بأن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية سيساعد الدول مساعدة كبيرة في تعزيز تشريعاتها التي تحكم استخدام أساليب التوثيق الحديثة وفي صياغة تشريعات من هذا القبيل حيثما لا توجد حاليا.

وإذ تـري أن إنشاء تشريعات نموذجية لتيسير استخدام التوقيعات الإلكترونية على نحو مقبول لدى الدول التي لها نظم قانونية واجتماعية واقتصادية مختلفة، يمكن أن يساهم في تطوير علاقات اقتصادية دولية متسقة.

١- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، بصيغته الواردة في المرفق الثاني من تقرير لجنة الأمم المتحدة للقانون التجاري

الدولي عن دورتها الرابعة والثلاثين<sup>(١)</sup>، مشفوعا بدليل اشتراع القانون النموذجي.

٢- تطلب إلي الأمين العام أن يحيل نص قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، مشفوعا بدليل اشتراع القانون النموذجي، إلي الحكومات والهيئات المهمة الأخرى.

٣- توصي جميع الدول بإيلاء نظرة إيجابية إلي قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية المعتمد حديثا، إلي جانب قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية المعتمد في سنة ١٩٩٦ والمستكمل في سنة ١٩٩٨، عندما تسن أو تتقح قوانينها، نظرا لضرورة توحيد القانون المطبق علي بدائل أشكال الاتصال الورقية وخزن المعلومات وتوثيقها<sup>(٢)</sup>.

ثانيا: القانون النموذجي كأداة للمواءمة بين القوانين:

٢٦- يتخذ القانون النموذجي الجديد، مثله مثل قانون الأونسيترال بشأن التجارة الإلكترونية، شكل نص تشريعي موصي به للدول لإدراجه في صلب قوانينها الوطنية، ولا يقصد من القانون النموذجي التدخل في الأعمال العادي لقواعد القانون الدولي الخاص (انظر أناه، الفقرة ١٣٦). وخلافا للاتفاقيات الدولية، لا يتطلب التشريع النموذجي من الدولة التي تشترعه إبلاغ الأمم المتحدة أو الدول الأخرى التي يمكن أن تكون قد اشترعته أيضا. غير أن الدول تشجع بقوة علي أن تبلغ أمانة الأونسيترال بأي اشتراع للقانون النموذجي الجديد (أو أي قانون نموذجي آخر ناتج عن أعمال الأونسيترال).

(1) المرجع نفسه، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17)، الفقرات ١٠٤ و ٢٣٨ و ٢٧٤ و ٢٨٣.  
(2) المرجع نفسه، الفقرة ٢٨٤.

٢٧- ويمكن للدولة، لدى إدراك نص التشريع النموذجي في صلي نظامها القانوني أن تعدل أو تهمل بعض أحكامه. أما في حالة الاتفاقيات، فإن إمكانية قيام الدول الأطراف بإجراء تغييرات في النص الموحد (ويشار إلى تلك التغييرات عادة بعبارة تحفظات) تكون أكثر تقييداً، وعادة ما تخطر اتفاقيات القانون التجاري، علي وجه الخصوص، التحفظات كلية أو تسمح بتحفظات محددة قليلة جداً. والمرونة التي تتميز بها التشريعات النموذجية مستصوبة بوجه خاص في الحالات التي يحتمل فيها أن ترغب الدول في إجراء تعديلات مختلفة للنص الموحد قبل أن تكون علي استعداد لاشتراكه كقانون وطني. ويمكن خصوصاً في توقيع إجراء بعض التعديلات عندما يكون النص الموحد وثيق الصلة بالنظام القضائي والإجرائي الوطني. غير أن ذلك يعني أيضاً أن درجة المواءمة التي تتحقق عن طريق التشريع النموذجي، ومدى اليقين بشأن تلك المواءمة، يحتمل أن يكونا أقل مما يكونان عليه في حالة الاتفاقية. بيد أن هذه المتطلبات النسبية للتشريع النموذجي يمكن أن توازن باحتمال كون عدد الدول التي تسن التشريع النموذجي أكبر من عدد الدول التي تنظم إلى الاتفاقية. ومن أجل تحقيق درجة مرضية من المواءمة واليقين، يوصي بأن تجري الدول أقل ما يمكن من التعديلات لدى إدراج القانون النموذجي الجديد في نظمها القانونية، وأن تراعي علي النحو الواجب مبادئه الأساسية، بما فيها الحياد إزاء التكنولوجيات، وعدم التمييز بين التوقيعات الإلكترونية المحلية والأجنبية، وحرية الأطراف، والمنشأ الدولي للقانون النموذجي. وعموماً يستصوب، لدى اشتراع القانون النموذجي الجديد (أو قانون الأونسيرال النموذجي بشأن التجارة الإلكترونية)، الالتزام قدر الإمكان بالنص الموحد، بغية جعل القانون الوطني شفافاً ومألوف قدر الإمكان لمستعملي القانون الوطني الأجانب.

٢٨- وجدير بالملاحظة أن بعض البلدان تعتبر أن المسائل القانونية ذات الصلة باستعمال التوقيعات الإلكترونية قد سبق حلها في قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، ولا تعترم اعتماد قواعد أخرى بشأن التوقيعات الإلكترونية علي أن تصبح الممارسات السوقية في هذا المجال الجديد أكثر رسوخا. بيد أنه يمكن للدول التي تشترع القانون النموذجي الجديد علي جانب قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية أن تتوقع منافع إضافية. فبالنسبة إلي البلدان التي تقوم السلطات الحكومية والتشريعية فيها بإعداد تشريعات بشأن مسائل التوقيعات الإلكترونية، بما في ذلك إنشاء مرافق مفاتيح عمومية، توفر أحكام معينة من القانون النموذجي توجيهها مستمدا من صك دولي أعد علي أساس وضع مسائل مرافق المفاتيح العمومية ومصطلحات مرافق المفاتيح العمومية نصب العين. وأما بالنسبة إلي جميع البلدان، فيوفر القانون النموذجي مجموعة من القواعد الأساسية التي يمكن تطبيقها خارج نطاق نموذج مرافق المفاتيح العمومية، لأنها تتوحي التفاعل بين وظيفتين متميزتين تتوافران في أي نوع من أنواع التوقيعات الإلكترونية (أي إنشاء التوقيع الإلكتروني والتعويل عليه)، ووظيفته ثالثة توجد في أنواع معينة من التوقيعات الإلكترونية (أي التصديق علي التوقيع الإلكتروني) وينبغي تناول تلك الوظائف الثلاث بغض النظر عما إذا كانت تؤديها في الواقع ثلاث هيئات منفصلة أو أكثر (كما في الحالة التي تنقسم فيها هيئات مختلفة جوانب مختلفة من وظيفة التصديق) أو إذا كان يؤدي اثنين من تلك الوظائف الشخص نفسه (كما في الحالة التي يؤدي فيها طرف معول وظيفة التصديق). وهكذا فإن القانون النموذجي يوفر أساسا مشتركا لنظم مرافق المفاتيح العمومية التي تعول علي سلطات تصديق مستقلة ونظم توقيعات إلكترونية لا تقوم فيها تلك الأطراف الثلاثة المستقلة باشتراك في عملية التوقيع الإلكتروني. وفي جميع الحالات يوفر القانون النموذجي الجديد

يقينا-إضافيا بشأن المفعول القانوني للتوقيعات الإلكترونية، بدون أن يحد من توافق المعيار المرن المتجسد في المادة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (انظر الفقرات ٦٧ و ٧٠ إلى ٧٥ ألتاه).

ثالثا: ملاحظات عامة بشأن التوقيعات الرقمية<sup>(١)</sup>:

#### أ- وظائف التوقيعات:

٢٩- تستند المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية إلى الاعتراف بوظائف التوقيع في بيئة ورقية ولدى أعداد قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، ناقش الفريق العامل الوظائف التالية التي تؤديها التوقيعات الخطية عادة: تحديد هوية الشخص، وتوفير ما يؤكد يقينا مشاركة ذلك الشخص بعينه في عملية التوقيع، والربط بين ذلك الشخص ومضمون المستند. بالإضافة إلى ذلك، لوحظ أن التوقيع يمكن أن يؤدي مجموعة متنوعة من الوظائف حسب طبيعة المستند الذي يحمل التوقيع. فعلى سبيل المثال، يمكن أن يكون التوقيع شاهدا على نية الطرف الالتزام بمضمون العقد الموقع عليه، وعلى نية الشخص الإقرار بتحريره النص (وبذلك يبين إدراكه لإمكانية ترتب نتائج قانونية على عملية التوقيع)، وعلى نية الشخص تأييد مضمون مستند كتبه شخص آخر، وعلى وجود شخص ما في مكان معين ووقت وجوده فيه. ويرد ألتاه في الفقرات ٦٥ و ٦٧ و ٧٠ إلى ٧٥ من هذا الدليل مزيد من المناقشة حول علاقة القانون النموذجي الجديد بالمادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية.

٣٠- في البيئة الإلكترونية، لا يمكن التمييز بين الرسالة الأصلية ونسخة منها، عندما لا تحمل الرسالة أي توقيع خطي ولا تكون مدونة على ورق.

(١) هذا الجزء مستمد من الوثيقة A/CN.9/WG.IV/WP.71، الجزء الأول.

كما أن إمكانية الغش كبيرة نظرا لسهولة اعتراض المعلومات المتوفرة في شكل إلكتروني وتغييرها دون اكتشاف ذلك، ونظرا للسرعة التي يمكن بها تجهيز معاملات متعددة، لذا فإن الغرض من التقنيات المختلفة المتوفرة في الأسواق في الوقت الحاضر، أو زالت قيد التطوير، هو إتاحة الوسائل التقنية التي يمكن بها أن يؤدي، في بيئة إلكترونية، بعض أو جميع الوظائف التي يتحدد أنها من خصائص التوقيعات الخطية، ويمكن أن يشار إلي هذه التقنيات بصورة عامة بعبارة "توقيعات إلكترونية".

#### ب- التوقيعات الرقمية وغيرها من التوقيعات الإلكترونية:

٣١- لدى مناقشة استصواب وجنوى إعداد القانون النموذجي الجديد، ولدى تحديد نطاق القواعد الموحدة بشأن التوقيعات الإلكترونية، درست الأونسيترال تقنيات التوقيعات الإلكترونية المختلفة المستخدمة حاليا أو التي لا تزال قيد التطوير، الغرض المشترك لتلك التقنيات هو إيجاد نظائر وظيفية لما يلي (أ) التوقيعات الخطية و (ب) الأنواع الأخرى من آليات التوثيق المستخدمة في بيئة ورقية (مثل وضع الأختام أو الطوابع). مستمدة من وظائف التوقيع ولكنها لا وجد لها نظير علي وجه الدقة في البيئة الورقية.

٣٢- كما هو مشار إليه أعلاه (انظر الفقرتين ٢١ و ٢٨) ينظر الإرشاد من الأونسيترال ، في بلدان عديدة، من جانب السلطات الحكومية والتشريعات التي تقوم بإعداد تشريعات بشأن مسائل التوقيعات الإلكترونية، بما في ذلك إنشاء مرافق مفاتيح عمومية أو مشاريع أخرى تتعلق بمسائل وثيقة الصلة بذلك (انظر الوثيقة A/ CN. 9/457، الفقرة ١٦). أما بشأن القرار الذي اتخذته الأونسيترال بالتركيز علي مسائل مرافق ومصطلحات المفاتيح العمومية، فينبغي أن يلاحظ أن تفاعل العلاقات بين ثلاثة أنواع متميزة من الأطراف (وهي الموقعون موردين خدمات التصديق والأطراف المعولة) يناظر نمودجا ممكنا واحدا لمرافق المفاتيح العمومية ولكن هناك نماذج

أخرى شائعة الاستعمال من قبل في السوق (مثلا حيث لا يشارك في ذلك أي مقدم خدمات تصديق مستقل). ومن الفوائد الرئيسية التي تنبثق من التركيز على مسائل مرافق المفاتيح العمومية تيسير هيكل القانون النموذجي من التركيز على مسائل مرافق المفاتيح العمومية تيسير هيكل القانون النموذجي، وذلك بالإشارة إلى ثلاث وظائف (أو ثلاثة أدوار) فيما يتعلق بالتوقيعات الإلكترونية، هي وظيفة الموقع، ووظيفة التصديق، ووظيفة التعويل. وتشارك جميع نماذج مرافق المفاتيح العمومية في وظيفتين من تلك الوظائف (هما إنشاء التوقيع الإلكتروني والتعويل عليه) أما الوظيفة الثالثة فتوجد في العديد من نماذج مرافق المفاتيح العمومية (وهي وظيفة التصديق على التوقيع الإلكتروني). وينبغي تناول تلك الوظائف الثلاث بصرف النظر عما إذا كانت تقدمها في الواقع ثلاث هيئات مستقلة أو أكثر (وذلك، مثلا، عندما تقتسم هيئات مختلفة جوانب شتى من وظيفة التصديق). أو ما إن كان الشخص نفسه يؤدي اثنتين من تلك الوظائف (وذلك، مثلا، عندما يكون مقدم خدمات التصديق هو أيضا طرف معول). علما بأن التركيز على الوظائف التي تؤدي في بيئة مرافق المفاتيح، وليس على أي نموذج محدد، ييسر أيضا وضع قواعد محايدة تماما لجزاء الوسائط، إلى حد أنه يمكن لوظائف مماثلة أن تؤدي بتكنولوجيا غير تكنولوجيا التوقيعات الإلكترونية الخاصة بمرافق المفاتيح العمومية.

١- التوقيعات الإلكترونية المعتمدة على تقنيات أخرى غير الترميز بالمفتاح العمومي:

٣٣- إلى جانب "التوقيعات الرقمية" المستندة إلى الترميز بالمفتاح العمومي، توجد أدوات أخرى مختلفة يشملها أيضا المفهوم الأوسع لآليات "التوقيع الإلكتروني" ويمكن أن تكون مستخدمة في الوقت الحاضر أو ينظر في أمر استخدامها مستقبلا بهدف أداء وظيفة واحدة أو أكثر من الوظائف

الأثفة الذكر التي تؤديها التوقيعات الخطية. من الأمثلة على ذلك تقنيات معينة تعتمد على التوثيق بواسطة أداة قياس حيوي تستند إلى التوقيعات الخطية. وبهذه الأداة يوقع الموقع يدويا باستخدام قلم خاص أما على شاشة الحاسوب أو على لوح رقمي. وعندئذ يحلل التوقيع الخطي بواسطة الحاسوب ويخزن كمجموعة من القيم الرقمية التي يمكن أن تضاف إلى رسالة البيانات وأن يعرضها الطرف المعول على شاشة الحاسوب "لأغراض التوثيق". ويفترض نظام التوثيق هذا أن تكون عينات من التوقيع الخطي قد سبق تحليلها وتخزينها بواسطة أداة القياس الحيوي. وتشمل التقنيات الأخرى استخدام أرقام الهوية الشخصية ("PIN") والصيغ المرقمة للتوقيعات الخطية، وطرائق أخرى كالنقر على مربع الموافقة ("Ok-box").

٣٤- هذا، وكانت الأونسيترال تعترّم وضع تشريع موحد يمكن أن يبسر استخدام كل من التوقيعات الرقمية والأشكال الأخرى من التوقيعات الإلكترونية. ولبلّوغ تلك الغاية، سعت الأونسيترال إلى تناول المسائل القانونية المتعلقة بالتوقيعات الإلكترونية على مستوى وسط بين المستوى العالي من العمومية الذي يتسم به قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية؟، والتحديد الذي قد يلزم لدى تناول تقنية توقيع معينة. وأيا كان الأمر فإنّه، عملاً بالحياد إزاء الوسائط، المتبع في الأونسيترال النموذجي بشأن التجارة الإلكترونية، لا ينبغي تفسير القانون النموذجي الجديد على أنه يثبت العظم على استخدام أي طريقة من طرائق التوقيع الإلكتروني، سواء كانت موجودة بالفعل أم ستفد في المستقبل.

٢- التوقيعات الرقمية المعتمدة على الترميز بالمفتاح العمومي<sup>(١)</sup>:

(١) استند في عرض كثير من عناصر وصف أداء نظام التوقيع الرقمي في هذا الفرع إلى المبادئ التوجيهية للتوقيع الرقمي، الصادرة عن رابطة المحامين الأمريكيين، الصفحات من ٨ إلى ١٧.



٣٥- بالنظر إلى تزايد استخدام تقنيات التوقيع الرقمي في عدد من البلدان، يمكن أن يكون التمهيد التالي مفيداً.

#### (أ) المفاهيم والمصطلحات:

##### ١- الترميز:

٣٦- تنشأ التوقيعات الرقمية ويتحقق من صحتها باستخدام الترميز، وهو فرع الرياضيات التطبيقية الذي يعني بتحويل الرسائل إلى أشكال تبدو غير مفهومة ثم أعادتها إلى أشكالها الأصلية. وتستخدم التوقيعات الرقمية ما يعرف باسم "الترميز بالمفتاح العمومي" الذي كثيراً ما يستند إلى استخدام دوال خوارزمية لإنتاج مفتاحين مختلفين ولكنهما مترابطان رياضياً (والمفتاحين هي أعداد ضخمة يحصل عليها باستخدام سلسلة من الصيغ الرياضية المطبقة على أعداد أولية). يستخدم أحد هذين المفتاحين في إنشاء توقيع رقمي أو في تحويل بيانات إلى أشكال غير مفهومة في ظاهرها، ويستخدم المفتاح الثاني للتحقيق من صحة توقيع رقمي أو إعادة رسالة البيانات إلى شكلها الأصلي. وكثيراً ما يشار إلى الأجهزة والبرمجيات الحاسوبية التي تستخدم مثل هذين المفتاحين بعبارة جامعة هي "نظم ترميز" (Cryptosystems) أو بعبارة أكثر تحديداً هي "نظم ترميز غير متناظرة" (asymmetric Cryptosystems) حيث تعتمد على خوارزميات غير متناظرة.

٣٧- في حين أن استخدام الترميز هو أحد السمات الرئيسية للتوقيعات الرقمية فإن مجرد كون التوقيعات يستخدم لتوثيق رسالة تحتوي على معلومات مقننة في شكل رقمي ينبغي ألا يخلط بينه وبني الاستخدام الأعم ترميز لأغراض السرية. والترميز لأغراض السرية هو طريق تستخدم لترميز الاتصالات الإلكترونية بحيث لا يتمكن من قراءتها أحد غير منشئ الرسالة والمرسلة إليه. وفي عدد من البلدان، يفيد القانون استخدام الترميز

لأغراض السرية، وذلك لأسباب لها صلة بالسياسة العامة المنطوية علي اعتبارات الدفاع الوطني، من جهة أخرى، فإن استخدام الترميز لأغراض التوثيق بإنشاج توقيع رقمي لا يعني ضمنا بالضرورة استخدام الترميز لإضفاء السرية علي أي معلومات أثناء عملية الاتصال، نظر لأن التوقيع الرقمي المرمز قد لا يكون سوى إضافة إلي رسالة غير مرمزة.

## ٢- المفاتيح العمومية والخصوصية:

٣٨- المفتاحان اللذان يكمل أحدهما الآخر واللذان يستخدمان للتوقيعات الرقمية يعرف أحدهما باسم "المفتاح الخاص" وهو المفتاح الذي يستخدمه إلا الموقع في إنشاء توقيع رقمي، ويعرف الآخر باسم "المفتاح العمومي"، الذي يكون عادة معروفا علي نطاق أوسع، ويستخدمه طرف معول للتحقق من صحة التوقيع الرقمي، ويتوقع من مستعمل المفتاح الخاص أن يحافظ علي سرية ذلك المفتاح الخاص. وجدير بالملاحظة أن المستعمل الفرد لا يحتاج إلي معرفة المفتاح الخاص، فمن المحتمل أن يحفظ المفتاح الخاص علي "بطاقة ذكية"، أو أن يتاح النفاذ إليه عن طريق رقم لتحديد الهوية أو عن طريق أداة قياس حيوي لتحديد الهوية، وذلك مثلا عن طريق التعرف علي البصمات، وإذا احتاج عدد كبير من الناس إلي التحقق من صحة التوقيعات الرقمية للموقع، تعين إتاحة المفتاح العمومي لهم جميعا أو توزيعه عليهم بنشره، مثلا في مستودع تسجيل حاسوب للاتصال المباشر أو في أي دليل عمومي ذي شكل آخر يسهل الوصول إليه. وعلي الرغم من أن زوج المفاتيح مترابط رياضيا، فإن من المستحيل علميا استخراج المفتاح الخاص انطلاقا من معرفة المفتاح العمومي إذا صمم نظام الترميز ونفذ بطريقة مأمونة. وأكثر الخوارزميات شيوعا من أجل الترميز باستخدام المفتاحين العمومي والخصوصي تستند إلي سمة هامة من سمات الأعداد الأولية الكبيرة فما أن تضرب تلك الأعداد بعضها ببعض فتتاج عدد جديد

حتى يكون من الصعب ومن المستنزف للوقت بوجه خاص معرفة أي عديدين أوليين أنشأ ذلك الرقم الجديد الأكبر<sup>(١)</sup>. وهكذا، فعلي الرغم من أن أناسا عديدين قد يعرفون المفتاح العمومي لموقع معين ويستخدمه في التحقق من صحة توقعات ذلك الموقع، فإنه لا يمكنهم أن يكتشفوا المفتاح الخصوصي للموقع ويستخدموه في تزيف توقعات رقمية.

جدير بالذكر مع ذلك أن مفهوم الترميز بالمفتاح العمومي لا ينطوي بالضرورة علي استخدام الخوارزميات الأنفة الذكر المبينة علي الأعداد الأولية. وذلك أنه توجد في الوقت الراهن تقنيات رياضية أخرى تستخدم أو قيد التطوير، يذكر منها نظم الترميز التي تعتمد علي المنحنيات الأليلجية، والتي كثيرا ما يقال إنها تتيح درجة عليه من الأمان من خلال استخدام مفاتيح مخفضة الطول تخفيضاً كبيراً.

### ٣- دالة البعثة:

٤٠- إلي جانب عملية إنتاج أزواج المفاتيح، توجد عملية أساسية أخرى يشار إليها عموماً بعبارة "دالة البعثة" (hash function) وتستخدم في إنشاء التوقعات الرقمية وفي التحقق من صحتها، ودالة البعثة هي عملية رياضية مبينة علي خوارزمية تنشئ صورة رقمية للرسالة أو شكلاً مضغوطاً من الرسالة، كثيراً ما يشار إليهما بعبارة "خلال رسالة" (

---

(1) تشير بعض المعايير الموجودة، مثل "المبادئ التوجيهية للتوقعات الرقمية" الصادرة عن رابطة المحامين الأمريكيين إلي مفهوم "الاستحالة الحسابية" (computational infeasibility) لوصف أوقع عدم قابلية العملية للعكس، أي الأمل في استحالة اشتقاق المفتاح الخصوصي السري للمستعمل من المفتاح العمومي لذلك المستعمل، (والاستحالة الحسابية) مفهوم نسبي يستند إلي قيمة البيانات المحمية، وتكلف العمليات الحسابية اللازمة لحمايتها وطول الفترة التي تلزم حمايتها أثناءها، والتكلفة والوقت اللازمين للاعتداء علي البيانات، مع تقدير هذه العوامل علي ما هي عليه في الوقت الراهن وعلي ضوء التقدم التكنولوجي المقبل (المبادئ التوجيهية للتوقعات الرقمية، رابطة المحامين الأمريكيين، ص ٩، الملاحظة ٢٣).

message digest) أو 'بصمة رسالة' (message fingerprint) تتخذ شكل قيمة بعترة (hash value) أو 'نتيجة بعترة' (hash result) ذات طول موحد يكون عادة أصغر كثيرا من الرسالة ولكن تتفرد به الرسالة إلى حد كبير. وأي تغيير يطرأ على الرسالة تترب عليه دائما نتيجة بعترة مختلفة عندما تستخدم دالة البعترة نفسها. وفي حالة دالة بعترة مأمونة، تعرف أحيانا باسم 'دالة بعترة ذات اتجاه واحد'، "one-way hash function" يكون في حكم المستحيل فعليا استخراج الرسالة الأصلية انطلاقا من معرفة قيمة البعترة الخاصة بها. وعلى ذلك فإن دوال البعترة تمكن البرمجيات المعدة لإنشاء التوقيعات الرقمية من العمل بمقادير أصغر من البيانات التي يمكن التنبؤ بها، بينما توفر في الوقت ذاته ارتباطا استدلاليا قويا بمحتوي الرسالة الأصلية، وتوفر بالتالي تأكيدا كافيا على أنه لم يطرأ على الرسالة أي تعديل على الرسالة أي تعديل منذ أن وقعت رقميا.

#### ٤- التوقيع الرقمية:

٤١- عند التوقيع على مستند أو على أي معلومات أخرى، يبين الموقع بدقة أولا حدود ما يريد التوقيع عليه. ثم تتولي دالة بعترة في برمجيات الموقع حساب نتيجة بعترة تتفرد بها (لجميع الأغراض العملية) المعلومات التي يراد التوقيع عليها. وعندئذ تحول برمجيات الموقع نتيجة البعترة إلى توقيع رقمية باستخدام المفتاح الخصوصي للموقع وبذلك يكون التوقيع الرقمي الناتج عن ذلك توقيعاً تتفرد به المعلومات التي يجري التوقيع عليها والمفتاح الخصوصي الذي استخدم في إنشاء التوقيع الرقمي.

٤٢- من المعتاد أن يلحق التوقيع الرقمي (نتيجة بعترة للرسالة موقع عليها رقميا) بالرسالة ويخزن أو ينقل مع تلك الرسالة، غير أن من الممكن أيضا إرساله أو تخزينه على أنه عنصر بيانات منفصل، ما دام مرتبطا بالرسالة المناظر ارتباطا يمكن التعويل عليه. وبالنظر إلى أن التوقيع الرقمي

يخص الرسالة التي تحمله دون سواها، فإن لا يكون صالحا للاستعمال إذا فصل عن الرسالة بصفة دائمة.

#### ٥- التحقق من صحة التوقيع الرقمي:

٤٣- التحقق من صحة التوقيع الرقمي هو عملية تدقيق للتوقيع الرقمي بالرجوع إلى الرسالة الأصلية وإلى مفتاح عمومي معين للبت فيما إذا كان ذلك التوقيع الرقمي قد أنشئ لتلك الرسالة ذاتها باستخدام المفتاح الخصوصي المناظر للمفتاح العمومي المشار إليه. ويتم التثبيت من صحة التوقيع الرقمي بحساب نتيجة بعثرة جديدة للرسالة الأصلية بواسطة دالة البعثرة نفسها التي استخدمت لإنشاء التوقيع الرقمي. ثم يقوم المحقق، مستخدماً المفتاح العمومي ونتيجة البعثرة الجديدة، بالتدقيق فيما إذا كان التوقيع الرقمي قد أنشئ باستخدام المفتاح الخصوصي المناظر وما إذا كانت نتيجة البعثرة المحسوبة حديثاً تطابق نتيجة البعثرة الأصلية التي حولت إلى التوقيع الرقمي أثناء عملية التوقيع.

٤٤- وتؤكد برمجيات التحقق "صحة" التوقيع الرقمي إذا: استخدم المفتاح الخصوصي للموقع لتوقيع الرسالة رقمياً، وهو ما يحدث إذا استخدم المفتاح العمومي للموقع للتحقق من صحة التوقيع، لأن المفتاح العمومي للموقع لا يثبت إلا صحة توقيع رقمي أنشئ بواسطة المفتاح الخصوصي للموقع، و (ب) لم يطرأ على الرسالة أي تغيير، وهو ما يحدث إذا كانت نتيجة البعثرة التي حسبها المحقق مطابقة لنتيجة البعثرة المستخرجة من التوقيع الرقمي أثناء عملية التحقق من صحته.

#### (ب) مرافق المفاتيح العمومية وموردو خدمات التصديق:

٤٥- للتحقق من صحة توقيع رقمي، يجب أن يتاح للمحقق الوصول إلى المفتاح العمومي للموقع وأن يضمن له تناظره مع المفتاح الخصوصي للموقع

غير أنه ليس لزوج المفاتيح العمومي والخصوصي أي ارتباط جوهري بأي شخص معين، إذ أنه مجرد زوج من الأرقام. ومن الضروري توافر آلية إضافية لإقامة صلة يعول عليها بين شخص معين أو هيئة معينة وزوج المفاتيح. وإذا كان للترميز بالمفتاح العمومي أن يحقق الأغراض المقصود منه، كأن من الضروري تمهيد الطريق لإتاحة المفاتيح لطائفة متنوعة من الأشخاص الذين يكون كثيرون منهم غير معروفين لدى الموقع عندما لا تكون علاقة ثقة قد نشأت بين الأطراف، ولتحقيق هذه الغاية يجب أن تتوفر لدى الأطراف المعنية درجة من الثقة فيما يصدر من مفاتيح عمومية وخصوصية.

٤٦- وقد يتوافر مستوى الثقة المطلوب بين الأطراف التي تثق بعضها ببعض، أو تكون قد تعاملت فيما بينها طوال فترة من الزمن، أو تقيم اتصالات فيما بينها ضمن نظم مغلقة، أو تعمل داخل مجموعة مغلقة، أو لديها القدرة على تنظيم معاملاتها تعاقدية كأن يكون بينها مثلا اتفاق شراكة تجارية. أما في المعاملة التي لا تضم سوى طرفين، فإنه يمكن لكل طرف منهما أن يكتفي بإبلاغ الآخر (عبر قناة مأمونة نسبيا، مثل رسول أو هاتف، مع ما ينطوي عليه الهاتف من خاصية التعرف على الصوت) بالمفتاح العمومي من زوج المفاتيح الذي سيستخدمه. غير أنه قد لا يتوفر المستوى نفسه من الثقة عندما لا تتعامل الأطراف فيما بينها بصورة منتظمة أو لا تجري اتصالاتها على نظم مفتوحة (مثل شبكة الويب العالمية التي توفرها الإنترنت)، أولا تعمل في إطار مجموعة مغلقة، أو لا تكون لديها اتفاقات شراكة تجارية أو قانون آخر يحكم علاقاتها.

٤٧- علاوة على ذلك، وبالنظر إلى أن الترميز بالمفتاح العمومي هو تكنولوجيا رياضية معقدة، فإنه يجب أن تتوفر لجميع مستعمليه الثقة في

مهارة ومعرفة الأطراف التي تصدر المفاتيح العمومية والخصوصية وفي ما تتخذها تلك الأطراف من ترتيبات أمان<sup>(١)</sup>.

٤٨- وقد يصدر موقع مرتقب بياناً للجمهورية يذكر فيه أن التوقيعات التي يمكن التحقق من صحتها بمفتاح عمومي معين ينبغي أن تعامل على أنها ناشئة من ذلك الموقع. ويخضع شكل ذلك البيان وفاعليته القانونية لقانون الدولة المشترعة. والافتراض بأن توقيعات إلكترونية تعود إلى موقع معين يمكن إثباته، مثلاً، من خلال نشر بيان في جلسة رسمية أو في وثيقة تعترف السلطات العمومية بأنها "صحيحة" (انظر الوثيقة A/ CN. 9/484، الفقرة ٣٦). غير أن أطرافاً أخرى قد لا تكون على استعداد لقبول البيان وبخاصة إذا لم يكن قد أبرم عقد سابق يرسى، على وجه اليقين، المفعول القانوني لذلك البيان المنشور. فالطرف الذي يعول على مثل هذا البيان المنشور في نظام مفتوح ودون سند يدعمه، سيكون عرضة لمخاطرة كبيرة تتمثل في أن يضع ثقته، بدون قصد، في شخص محتال، أو أن يضطر إلى دحض إنكار باطل لتوقيع رقمي (وهي مسألة كثيراً ما يشار إليها في سياق "عدم الاتصال من التوقيعات الرقمية") إذ تبين أن معاملة ما ليست في صالح الموقع المزعوم.

٤٩- أحد أنواع الجدول لبعض هذه المشاكل هو استخدام طرف ثالث واحد أو أكثر للربط بين موقع محدد الهوية أو اسم الموقع من جهة، ومفتاح عمومي معين من الجهة الأخرى. ويشار إلى هذا الطرف الثالث عموماً بعبارة "سلطة التصديق" أو "مقدم خدمات التصديق" أو "مورد خدمات التصديق" في معظم المعايير والمبادئ التوجيهية التقنية (في القانون النموذجي، اختيرت عبارة "مقدم خدمات التصديق"). وفي عدد من البلدان،

(١) في المواقف التي يتولى فيها المستعملون أنفسهم إصدار مفاتيح الترميز العمومية والخصوصية، قد يتعين قيام سلطات التصديق على المفاتيح العمومية بتوفير هذه الثقة.

تنظم سلطات التصديق هذه هرميا لتصبح ما يشار إليه في أحيان كثيرة بعبارة "مرفق المفاتيح العمومية". ويمكن أن تشمل الحلول الأخرى، مثلا، الشهادات التي تصدرها أطراف معولة.

#### ١- مرفق المفاتيح العمومية:

٥٠- إن إنشاء مرفق المفاتيح العمومية هو وسيلة لتوفير الثقة:

(أ) بأن المفتاح العمومي لمستعمل ما لم يعث به وبأنه يناظر بالفعل المفتاح الخاصي لذلك المستعمل،

(ب) بأن تقنيات الترميز المستخدمة تقنيات سليمة. ولتوفير الثقة المبينة أعلاه، يمكن أن يقدم مرفق المفاتيح العمومية عددا من الخدمات تشمل ما يلي:

(أ) إدارة مفاتيح الترميز المستعملة لأغراض التوقيع الرقمي،

(ب) التصديق على أن مفتاحا عموميا معينا يناظر مفتاحا خاصيا،

(ج) توفير مفاتيح للمستعملين النهائيين،

(د) نشر دليل مأمون بالمفاتيح العمومية أو بالشهادات،

(هـ) إدارة الرموز المحددة للشخصية (كالبطاقات الذكية مثلا) التي

يمكنها تحديد هوية المستعمل بمعلومات هوية شخصية فريدة أو أن تنتج وتخزن المفاتيح الخصوصية الخاصة بالأفراد،

(و) التحقق من هوية المستعملين النهائيين وتزويدهم بالخدمات،

(ز) تقديم خدمات ختم الوقت.

(ح) إدارة مفاتيح الترميز المستخدمة لأغراض السرية حيثما يكون

استخدام هذه التقنية مأمونا به.



٥١- كثيرا ما يكون مرفق المفاتيح العمومية مستندا إلى مستويات هرمية مختلفة من السلطة. من أمثلة لذلك أن النماذج التي يجري النظر فيها في بلدان معينة لإنشاء مرافق مفاتيح عمومية ممكنة تشمل علي إشارات إلى المستويات التالية:

(أ) "سلطة رئيسية" (root authority) فريدة تصدق علي تكنولوجيا وممارسات جميع الأطراف المأنون لها بإصدار أزواج مفاتيح ترميز أو شهادات تتعلق باستخدام تلك الأزواج من المفاتيح، كما تسجل سلطات التصديق التابعة لها<sup>(١)</sup>،

(ب) سلطات تصديق مختلفة تحتل مستوى أدني من مرتبة "السلطة الرئيسية" وتصدق علي أن المفتاح العمومي لأحد المستعملين يناظر بالفعل المفتاح الخاص لذلك المستعمل (أي أنه لم يعث به)،

(ج) سلطات تسجيل محلية مختلفة تحتل مستوى أدني من مستوى سلطات التصديق وتتلقى الطلبات من المستعملين للحصول علي أزواج مفاتيح الترميز أو علي الشهادات المتعلقة باستخدام تلك الأزواج من المفاتيح، وتشرط إثبات هوية المستعملين المحتملين وتحقق من تلك الهوية. وفي بلدان معينة، يعترف قيام موثقي العقود بدور سلطات التسجيل المحلية أو بمساندة تلك السلطات في مهمتها.

٥٢- لكن المسائل المتعلقة بمرافق المفاتيح العمومية قد لا يكون تنسيقها علي الصعيد الدولي أمرا يسيرا. فتتطلب مرفق المفاتيح العمومية قد ينطوي علي مسائل تقنية متنوعة وعلي مسائل تتعلق بالسياسة العامة التي قد يكون

(١) مسألة ما إذا كان ينبغي أن تكون لدى الحكومة القدرة التقنية علي الاحتفاظ بالمفاتيح الخصوصية المستخدمة لأغراض السرية أو علي إعادة إنشاء تلك المفاتيح هي مسألة يمكن تناولها علي مستوى السلطة الرئيسية.

من الأصوب ترك أمرها في المرحلة الحالية لكل دولة علي حدة<sup>(١)</sup>. وفي هذا الصدد، قد يكون من الضروري أن تقوم كل دولة بتتظر في إنشاء مرفق مفاتيح عمومية باتخاذ قرارات بشأن أمور منها مثلا:

(أ) شكل مرفق المفاتيح العمومية وعدد مستويات السلطة التي يشملها،  
(ب) ما إذا كان لا يسمح إلا لسلطات تصديق معينة تنتمي إلي مرفق المفاتيح العمومية بإصدار أزواج مفاتيح الترميز أو ما إذا كان من الممكن أن يصدر المستعملون أنفسهم تلك الأزواج من المفاتيح،  
(ج) ما إذا كانت سلطات التصديق التي تشهد بصحة أزواج مفاتيح الترميز ينبغي أن تكون هيئات عمومية أو أن من الممكن قيام هيئات خاصة بالعمل كسلطات تصديق،

(د) ما إذا كانت عملية السماح لهيئة معينة بالعمل بصفة مقدم خدمات تصديق ينبغي أن تتخذ شكل إذن صريح أو "ترخيص"، من الدولة، أو ما إذا كان ينبغي اللجوء إلي طرق أخرى لمراقبة نوعية سلطات التصديق ن هي سمح لها بالعمل دون الحصول علي إذن محدد،  
(هـ) المدى الذي يمكن الذهاب إليه في الإنن باستخدام الترميز لأغراض السرية،

(و) ما إذا كان ينبغي أن يكون للسلطات الحكومية الحق في الوصول إلي المعلومات المرمزة، عبر آلية "لاستيداع المفاتيح" (Key escrow) لدى طرف ثالث إيداعا مشروطا، أو بوسيلة أخرى، ولا يتناول القانون النموذجي هذه المسائل.

---

(١) بيد أنه، في سياق التصديق المتبادل (Cross- certification) تؤدي ضرورة الصلاحية للعمل تبادليا علي الصعيد العالمي إلي ضرورة أن تكون مرافق المفاتيح العمومية المنشأة في مختلف البلدان قادرة علي تبادل الاتصالات فيما بينها.

٥٣- للربط بين زوج من المفاتيح وبين موقع مرتقب، يصدر مقدم خدمات التصديق (أو سلطة التصديق) شهادة هي عبارة عن سجل إلكتروني يبين مفتاحاً عمومياً إلى جانب اسم صاحب الشهادة، باعتباره "موضوع" الشهادة، وقد يؤكد أن الموقع المرتقب المحددة هويته في الشهادة هو حائز المفتاح الخصوصي المناظر. الوظيفة الرئيسية للشهادة هي ربط مفتاح عمومي معين. وبوسع "متلقي" الشهادة الراغب في التعويل على توقيع رقمي أنشأه الموقع المسمى في الشهادة أن يستعمل المفتاح العمومي المبين في الشهادة للتحقق من أن التوقيع الرقمي أنشئ باستخدام المفتاح الخصوصي المناظر. فإذا تكمل ذلك التحقق بالنجاح، توفر مستوى من اليقين يثبت أن التوقيع الرقمي أنشأه الموقع، وأن الجزء من الرسالة المستخدم في دالة البعثة (وبالتالي رسالة البيانات المناظرة) لم يعدل منذ أن وقع عليه رقمياً.

٥٤- لتأكيد صحة الشهادة فيما يتعلق بكل من محتواها ومصدرها، يوقع عليها مقدم خدمات التصديق رقمياً. ويمكن التحقق من صحة التوقيع على الشهادة من جانب مقدم خدمات التصديق مصدر الشهادة، باستخدام المفتاح العمومي الخاص بمقدم خدمات التصديق المبين في شهادة أخرى صادرة عن مقدم خدمات تصديق آخر (ربما كان- وإن لم يكن ذلك بالضرورة- أعلى منه مستوى في النظام الهرمي)، كما يمكن للشهادة الأخرى بدورها أن تؤثق باستخدام المفتاح العمومي المبين في شهادة غير تلك الشهادة، وهكذا دواليك، إلى أن يطمئن الشخص المعول على التوقيع الرقمي إلى صحة التوقيع بما فيه الكفاية ومن بني الطرق الأخرى للتحقق من صحة التوقيع الرقمي لمقدم خدمات التصديق، يمكن أن يسجل ذلك التوقيع الرقمي أيضاً في شهادة يصدرها مقدم خدمات التصديق نفسه، ويشار إليها أحياناً باسم "الشهادة

الرئيسية<sup>(١)</sup>، وفي كل من هذه الحالات، يجب علي مقدم خدمات التصديق المصدر للشهادة أن يوقع رقمياً علي شهادته أثناء فترة سريان الشهادة الأخرى المستخدمة في التحقق من صحة التوقيع الرقمي لمقدم خدمات التصديق. وبموجب قولتين يعني البلدان، يمكن أن يتمثل بناء الثقة في التوقيع الرقمي لمقدم خدمات التصديق عن طريق نشر المفتاح العمومي الخاص بمقدم خدمات التصديق (انظر الوثيقة A/ CN. 9/484، الفقرة ٤١) أو بعض البيانات المتعلقة بالشهادة الرئيسية (مثل "البصمة الرقمية") في جلسة رسمية.

٥٥- أما التوقيع الرقمي المناظر لرسالة ما، سواء أنشأه الموقع لتوثيق رسالة، أو أنشأه مقدم خدمات تصديق لتوثيق شهادته، فينبغي عموماً أن يختم زمنياً علي نحو يعول عليه، لكي يتاح للمحقق أن يحدد بما لا يدع مجالاً للشك ما إذا كان التوقيع الرقمي قد أنشئ أثناء فترة السريان "المذكورة في الشهادة، وهذا شرط من شروط إمكانية التحقق من صحة التوقيع الرقمي.

٥٦- ولتيسير التحقق من صحة المفتاح العمومي وتناظره مع موقع معين، يمكن نشر الشهادة في مستودع تسجيل حاسوبي أو إتاحة الإطلاع عليها بوسائل أخرى. ومن الناحية النموذجية، تكون مستودعات التسجيل الحاسوبي قواعد بيانات للاتصال الحاسوبي المباشر تحوي الشهادات والمعلومات الأخرى المتاحة للاسترجاع والاستخدام في التحقق من صحة التوقيعات الرقمية.

٥٧- ربما يتبين، بعد إصدار الشهادة، أنه لا يعول عليها، كما يحدث في الحالات التي يقدم فيها الموقع إلي مقدم خدمات التصديق هوية غير هويته. وفي ظروف أخرى قد يكون من الممكن التعويل علي الشهادة حين صدورها، ولكنها تفقد إمكانية التعويل عليها بعد ذلك. فإذا تعرض المفتاح الخصوصي لما

(١) الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17)، الفقرة ٢٧٩.

يُشير الشبهة، كأن يفقد الموقع سيطرته علي ذلك المفتاح الخصوصي، فإن الشهادة قد تفقد جدارتها بالثقة أو تصبح غير قابلة للتعويل عليها، وقد يعد مقدم خدمات التصديق (بناء علي طلب الموقع حتى بدون موافقته، رهنا بالظروف) إلي تعليق الشهادة (بوقف فترة سريانها مؤقتاً) أو إلي إلغائها (إبطالها بصفة دائمة). وفور تعليق الشهادة أو إلغائها، يمكن أن يتوقع من مقدم خدمات التصديق أن ينشر إشعاراً بالإلغاء أو التعليق أو أن يبلغ الأمر إلي المستفسرين أو إلي الأشخاص الذين يعرف أنهم تلقوا توقيعاً رقمياً يمكن التحقق من صحته بالرجوع إلي الشهادة التي لا يمكن التعويل عليها.

٥٨- ويمكن أن تقوم جهات حكومية أو مقدمو خدمات في القطاع الخاص بالعمل كسلطات تصديق، ومن المتوقع في عدد من البلدان، لأسباب تتعلق بالسياسة العامة، أن لا يؤذن إلا الهيئات الحكومية بالعمل كسلطات تصديق، ويرى في بلدان أخرى أن خدمات التصديق ينبغي أن تكون مفتوحة للمنافسة من جانب القطاع الخاص. وبصرف النظر عما إذا كانت هيئات حكومية أو مقدمو خدمات في القطاع الخاص تضطلع بعمل سلطات التصديق، وعما إذا كانت سلطات التصديق ستحتاج أو لن تحتاج إلي الحصول علي رخصة للعمل، يوجد عادة أكثر من مقدم خدمات تصديق يعمل ضمن مرفق المفاتيح العمومية. وتشكل العلاقات بين سلطات التصديق المختلفة موضع قلق خاص. فسلطات التصديق الموجودة في مرفق المفاتيح العمومية يمكن إنشاؤها في بنية هرمية حيث تقتصر بعض سلطات التصديق علي اعتماد سلطات تصديق أخرى تقدم الخدمات مباشرة علي المستعملين. وفي بنية كهذه، تكون سلطات التصديق تابعة لسلطات تصديق أخرى. وفي بني أخرى يمكن تصورها، يمكن أن تعمل جميع سلطات التصديق علي قدم المساواة بعضها مع البعض الآخر. وفي أي مرفق كبير للمفاتيح العمومية، يرجح أن توجد سلطات تصديق تابعة وسلطات تصديق أعلي مستوى. وأياً

كان الأمر، ففي حال عدم وجود مرفق دولي للمفاتيح العمومية. قد ينشأ عند من دواعي القلق فيما يتعلق بالاعتراف بالشهادات التي تصدرها سلطات تصديق في بلدان أجنبية، وكثيراً ما يتم الاعتراف بالشهادات الأجنبية بواسطة طريقة تعرف باسم "التصديق المتبادلة" (Cross certification). ومن الضروري في مثل هذه الحالة أن تقوم سلطات التصديق المتكافئة إلى حد كبير (أو سلطات التصديق التي لديها الاستعداد ل تحمل مخاطر معينة فيما يتعلق بالشهادات الصادرة عن سلطات تصديق أخرى بالاعتراف بالخدمات التي تقدمها كل منها)، لكي يستطيع المنتفعون بخدمات كل منها أن يقيموا الاتصالات فيما بينهم على نحو أكثر كفاءة وأكبر يقيناً إزاء موثوقيه الشهادات التي يجري إصدارها.

٥٩- قد تنشأ مسائل قانونية فيما يتعلق بالتصديق المتبادل أو الربط بين سلسلة من الشهادات (Chaining of certification) عندما تنتهج سياسات أمان متعددة من الأمثلة على هذه المسائل، البت فيمن كان سوء سلوكه هو السبب في وقوع الخسارة، وتحديد التأكيدات التي اعتمد عليها المنتفع بالخدمات. ومن الجدير بالذكر أن القواعد القانونية التي يجري النظر في اعتمادها في بلدان معينة تنص على أنه حيث يبلغ المنتفعون بمستويات الأمان وبالسياسات المنتهجة، وحيث لا يقع إهمال من حيث يبلغ المنتفعون بمستويات الأمان وبالسياسات المنتهجة، وحيث لا يقع إهمال من جانب سلطات التصديق، لا ينبغي أن يتحمل أحد أي مسؤولية.

٦٠- وقد يتعين على كل من مقدم خدمات التصديق أو السلطة الرئيسية أن يكفل أن الشروط التي تقتضيها سياسته العامة يجري الوفاء بها على أساس مستمر. ففي حين أن اختيار سلطات التصديق قد يتوقف على عدد من العوامل، منها قوة المفتاح العمومي الذي يجري استعماله وهوية مستعملة، فإن الجدارة بالنقطة التي يتمتع بها أي مقدم خدمات تصديق قد تتوقف أيضاً

علي إنفاذه معايير إصدار الشهادات ومدى إمكانية التعويل علي تقييمه للبيانات التي يتلقاها من المستعملين الذين يطلبون الشهادات. والأمر الذي يتسم بأهمية بالغة هو نظام المساعلة الذي يضبط علي أي مقدم خدمات تصديق فيما يتعلق بقيامه باستمرار بالامتثال لشروط السياسة العامة والأمان الصادرة عن السلطة الرئيسية أو عن مقدم خدمات التصديق الأعلى مستوى، أو بالامتثال لأي شروط أخرى منطقية. والأمر الذي يتسم بأهمية مساوية هو التزام مقدم خدمات التصديق بأن يتصرف وفقا للتأكدات التي يقدمها بشأن سياسته وممارساته علي النحو المتوخي في المادة ٩ (١) (أ) من القانون النموذجي (انظر الوثيقة A/ CN. 9/484K، الفقرة ٤٣).

٦١- ولدى إعداد القانون النموذجي، جري النظر في العناصر التالية باعتبارها عوامل يمكن أن توضع في الاعتبار عند تقدير دارة مقدم خدمات التصديق بالنقطة:

- (أ) استقلاله (أي أنه ليست له أي مصالح مالية أو غيرها من المصالح في المعاملات الأصلية.
- (ب) موارده المالية وقدرته المالية علي تحمل المخاطر الناجمة عن تحمله مسئولية الخسارة،
- (ج) خبرته المتخصصة ي تكنولوجيا المفاتيح العمومية وإلمامه بإجراءات الأمن السليمة،
- (د) طول مدة بقائه في المستقبل (يمكن أن يطلب من سلطات التصديق تقديم إثباتات تصديق أو مفاتيح ترميز بعد منذ سنوات عديدة علي إتمام المعاملة الأصلية، وذلك في سياق دعوى قضائية أو مطالبة بملكية)،
- (هـ) الموافقة علي المعدات والبرمجيات.

(و) المحافظة علي سجل لمراجعة الحسابات وعلي إجراء مراجعة حسابات من جانب هيئة مستقلة،  
(ز) وجود خطة طوارئ (مثال ذلك وجوب برمجيات "استرداد المعلومات في حالات الكوارث"، أو آلية لاسترداد المفاتيح لدى طرف ثالث)،  
(ح) اختيار الموظفين وإدارتهم.  
(ط) ترتيبات الحماية اللازمة للمفتاح الخصوصي لمقدم خدمات التصديق ذاته.

(ي) الأمن الداخلي،  
(ك) ترتيبات إنهاء العمليات، بما في ذلك إشعار المستعملين،  
(ل) الضمانات والتأكيدات (المعطاة أو المستبعدة)،  
(م) حدود المسؤولية،  
(ن) التأمين،  
(ص) قابلية العمل تبادلياً مع سلطات التصديق الأخرى،  
(ع) إجراءات الإلغاء (في حالة ضياع مفاتيح الترميز أو تعرضها لما يثير الشبهة).

**(ج) ملخص عملية التوقيع الرقمي:**

٦٢- ينطوي استخدام التوقيعات الرقمية عادة علي العمليات التالية التي يؤديها إما الموقع أو متلقي الرسالة الموقع عليها رقمياً:  
(أ) ينتج المستعمل أو يتلقي زوجاً فريداً من مفاتيح الترميز،  
(ب) يعد الموقع رسالة علي حاسوب (في شكل رسالة بريد إلكتروني مثلاً)،



(ج) يعد الموقع "خلاصة رسالة" باستخدام خوارزمية بعبثرة مأمونة. وتستخدم في إنشاء التوقيع الرقمي نتيجة بعبثرة متأتية من الرسالة الموقع وتخصصها وحدها،

(د) يرمز الموقع خلاصة الرسالة باستخدام المفتاح الخصوصي. ويطلق المفتاح الخصوصي علي نص خلاصة الرسالة باستخدام خوارزمية رياضية، ويتألف التوقيع الرقمي من خلاصة مرزمة للرسالة،

(هـ) يرفق الموقع توقيع الرقمي عادة بالرسالة أو يلحقه بها،

(و) يرسل الموقع الرقمي ورسالته (غير المرزمة أو المرزمة) إلكترونيا علي الطرف المعول،

(ز) يستخدم الطرف المعول المفتاح العمومي للموقع للتحقق من صحة التوقيع الرقمي للموقع. والتحقق من الصحة باستخدام المفتاح العمومي للموقع يوفر مستوى من التأكيد التقني بأن الرسالة جاءت من الموقع دون سواء،

(ح) ينشئ الطرف المعول أيضا "خلاصة رسالة" للرسالة باستخدام نفس خوارزمية البعبثرة المأمونة،

(ط) يقارن الطرف المعول بين خلاصتي الرسالة، فإذا كانتا متطابقتين عرف الطرف المعول أن الرسالة لم تتغير بعد توقيعها حتى إذا لم يتغير سوى "بت" (رقم ثنائي) واحد في الرسالة بعد أن وقعت رقميا، ستكون خلاصة الرسالة التي أنشأها الطرف المعول مختلفة عن خلاصة الرسالة التي أنشأها الموقع،

(ي) في حالة اللجوء إلي عملية التصديق، يحصل الطرف المعول علي شهادة من مقدم خدمات التصديق (بما في ذلك عن طريق الموقع أو بصورة أخرى) تؤكد التوقيع الرقمي علي رسالة الموقع (انظر الوثيقة A/ CN. 9/484، الفقرة ٤٤). وتحتوي الشهادة علي المفتاح العمومي واسم الموقع

وربما معلومات إضافية)، موقعا عليهما رقميا من جانب مقدم خدمات التصديق.

رابعاً: السمات الرئيسية في القانون النموذجي:

أ- الطابع التشريعي للقانون النموذجي:

٦٣- أعد القانون النموذجي الجديد بناء على الافتراض القائل بأنه ينبغي أن يكون هذا القانون مستندا مباشرة من المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، وينبغي أن يعتبر وسيلة لتقديم معلومات تفصيلية بشأن مفهوم العبارة "طريقة لتحديد هوية الشخص" جدير بالتعويل عليها" و "التدليل على موافقة ذلك الشخص" على المعلومات الواردة في رسالة البيانات (انظر A/CN.9/WG.IV/WP.71، الفقرة ٤٩).

٦٤- وقد أثارت مسألة الشكل الذي يمكن أن يتخذه الصك، كما أشير إلى أهمية النظر في علاقة الشكل بالمضمون. فاقترحات نهج مختلفة بشأن الشكل الجائز، ومنها القواعد التعاقدية، أو الأحكام التشريعية، أو المبادئ التوجيهية للدول التي تنظر في سن تشريعات بشأن التوقيعات الإلكترونية. واتفق، بصفة افتراض عملي، على أن يعد النص باعتباره قواعد تشريعية مشفوعة بتعليق، لا باعتباره مبادئ توجيهية فحسب (انظر A/ CN. 9/437، الفقرة ٢٧، A/ CN. 9/446، الفقرة ٢٥، A/ CN. 9/457، الفقرتين ٥١ و ٧٢). وأخيراً اعتمد النص كقانون نموذجي (A/ CN. 9/483، الفقرتان ١٣٧ و ١٣٨).

ب- العلاقة بقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية:

١- القانون النموذجي الجديد باعتباره صكاً قانونياً منفصلاً:

٦٥- كان يمكن إدراج الأحكام الجديدة في صيغة موسعة لقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لتشكيل على سبيل المثال

جزءاً جديداً ثالثاً من قانون الأونسيترال النموذجي الجديد يمكن اشتراعه إما مستقلاً وإما مقترناً بقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، تقرر في نهاية المطاف أن القانون النموذجي الجديد ينبغي أن يعد بصفة صك قانوني منفصل (انظر الوثيقة A/ CN. 9/465، الفقرة ٣٧). وهذا القرار ناشئ أساساً من أنه، في وقت وضع القانون النموذجي في صيغته النهائية كان قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية قد نفذ بنجاح في عدد من البلدان وكانت بلدان أخرى كثيرة تنتظر في اعتماده، وكان يمكن أن يؤدي إعداد صيغة موسعة لقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية إلى المساس بنجاح الصيغة الأصلية، وذلك بالإيحاء بوجود حاجة إلى إجراء تحسين لذلك النص بإصدار صيغة حديثة العهد. وفضلاً عن ذلك فإن إعداد صيغة جديدة لقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية كان يمكن أن يسبب تشويشاً في البلدان التي اعتمدت قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مؤخراً.

## ٢- القانون النموذجي الجديد متسق تماماً مع الأونسيترال النموذجي بشأن التجارة الإلكترونية:

٦٦- لدى صياغة القانون النموذجي الجديد، بذل كل جهد لضمان الاتساق مع مضمون قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية ومصطلحات (A/ CN. 9/465، الفقرة ٣٧). وقد نقلت إلى الصك الجديد الأحكام العامة لقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. وهذه الأحكام هي المواد ١ (نطاق التطبيق)، ٢ (أ) و (ج) و (د) (تعريف المصطلحات "رسالة بيانات" و "منشئ رسالة البيانات" و "المرسل إليه")، و ٣ (التفسير)، و ٤ (التغيير بالاتفاق) و ٧ (التوقيع)، من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية.

٦٧- وإذ يستند القانون النموذجي الجديد إلى قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، فإنه يقصد منه أن يجسد على الخصوص ما يلي: مبدأ الحياد بين الوسائط، وأنباع نهج يستوجب عدم التمييز تجاه استعمال النظائر الوظيفية للمفاهيم والممارسات الورقية التقليدية، والاعتماد الواسع النطاق على حرية الأطراف A/CN.9/WG.IV/WP.84 ، (الفقرة ١٦). والمقصود أيضا أن يستخدم القانون النموذجي الجديد كمعايير دنيا في بيئة "مفتوحة" (أي حيث يتصل الأطراف فيما بينهم إلكترونيا دونما اتفاق مسبق) وكذلك، عند الاقتضاء، كأحكام تعاقدية نموذجية أو كقواعد مفترضة احتياطيا في بيئة "مغلقة" (أي حيث يكون الأطراف ملزمين بقواعد وإجراءات تعاقدية موجودة مسبقا ينبغي اتباعها في الاتصال بالوسائل الإلكترونية).

### ٣- العلاقة بالمادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية:

٦٨- لدى إعداد القانون النموذجي الجديد، أبدى رأي مفاده أن الإشارة الواردة في نص المادة ٦ من القانون النموذجي الجديد إلى المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية ينبغي أن تفسر بأنها تقصر نطاق القانون النموذجي الجديد على الأحوال التي يستخدم فيها توقيع الإلكتروني لتلبية شرط قانوني إلزامي يقضي بأن مستندات معينة ينبغي أن يوقع عليها لأغراض تبين صلاحياتها وذهب ذلك الرأي إلى أن نطاق القانون النموذجي الجديد بالضييق، بالنظر إلى أن القانون في معظم الدول لا يحتوي إلا على شروط قليلة للغاية بشأن المستندات التي تستخدم في المعاملات التجارية، وردا على ذلك، اتفق عموما على أن ذلك التفسير لمشروع المادة ٦ (والمادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية) يتتافي مع تفسير عبارة "القانون" الذي اعتمدته اللجنة في الفقرة

٦٨ من دليل تشريع قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، والذي ينص علي أنه "ينبغي أن تفهم الكلمة "القانون"... وعلي إنها لا تشمل القانون التشريعي أو القانون التنظيمي فحسب، بل تشمل أيضا القانون القضائي المنشأ والقوانين الإجرائية الأخرى". والواقع أن نطاق المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية ونطاق المادة ٦ من القانون النموذجي الجديد كلاهما واسع بصفة خاصة، لأن معظم المستندات المستخدمة في سياق المعاملات التجارية يحتمل أن توجهها، في الممارسة العملية، الشروط الواردة في قانون البيانات بشأن إثبات كتابة ( A/ CN. 9/465، الفقرة ٦٧).

#### ج- قواعد اطارية تدعم باللوائح التنظيمية وبالتعاقد:

٦٩- يقصد من القانون النموذجي الجديد، باعتباره مكملا لقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، أن يقدم مبادئ جوهرية لتيسير استعمال التوقيعات الإلكترونية، غير أن القانون النموذجي نفسه، بصفته "إطار"، لا يضع جميع القواعد والأنظمة التي قد تلزم (علاوة علي الترتيبات التعاقدية بين المستعملين) لتنفيذ تلك التقنيات في الدولة المشترعة. فضلا عن ذلك، فكما هو مبين في الدليل، لا يقصد من القانون النموذجي أن يتناول كل جانب من جوانب استعمال التوقيعات الإلكترونية. بناء عليه فقد ترغب الدولة المشترعة في إصدار لوائح تنظيمية تتضمن تفاصيل للإجراءات التي ينص عليها القانون النموذجي، وتراعي الظروف المعينة السائدة، وربما المتغيرة في الدولة المشترعة، دون مساس بأهداف القانون النموذجي. ويوصي بأن تعني الدولة المشترعة عناية خاصة، إذ قررت إصدار تلك اللوائح، بالحاجة إلي الحفاظ علي المرونة في تشغيل نظم التوقيع الإلكتروني من جانب مستعملي تلك النظم. وتعتمد الممارسة التجارية منذ وقت ويل علي عملية المعايير التقنية الطوعية. وتشكل هذه المعايير التقنية

أسس مواصفات الإنتاج، والمعايير الهندسية ومعايير التصميم، وتوافق الآراء المتعلقة ببحث وتطوير المنتجات في المستقبل. ولكافة المرونة، التي تعتمد عليها هذه الممارسة التجارية، ولترويج المعايير المفتوحة بهدف تيسير القابلية للعمل المتبادل، ولدعم هدف الاعتراف عبر الحدود (علي النحو المبين في المادة ١٢)، قد ترغب الدول أن تتولي الاعتبار الواجب للعلاقة بين أي مواصفات مدرجة أو مأذون بها في النظم الوطنية، وعملية المعايير التقنية الطوعية (انظر الوثيقة A/ CN. 9/484، الفقرة ٤٦).

٧٠- وينبغي أن يلاحظ أن تقنيات التوقيع الإلكتروني التي يتناولها القانون النموذجي يمكن أن تثير، إلى كاتب المسائل الإجرائية التي قد يلزم التصدي لها لدى تنفيذ اللوائح التنظيمية التقنية، مسائل قانونية معينة لا تكون الإجابات عليها موجودة بالضرورة في القانون النموذجي بل في نصوص قانونية أخرى، قد يكون من تلك النصوص القانونية الأخرى مثلا القوانين الإدارية وقوانين العقود وقوانين الضرر والقوانين الجنائية والقوانين القضائية- الإجرائية المطبقة، التي لا يقصد من القانون النموذجي أن يتناولها.

#### د- مزيد من القين بشأن المفاعيل القانونية للتوقيعات الإلكترونية:

٧١- تتمثل إحدى السمات الرئيسية للقانون النموذجي في إضافة مزيد من اليقين إلى تطبيق المعيار المرن الوارد في المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية بخصوص الاعتراف بالتوقيع الإلكتروني باعتباره نظيرا وظيفيا للتوقيع الخطي. وفيما يلي نص المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية:

١- عندما يشترط القانون وجود توقيع من شخص، يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

(أ) استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل علي موافقة ذلك الشخص علي المعلومات الواردة في رسالة البيانات، أو  
(ب) كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله من رسالة البيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق متصل بالأمر.

٢) تسري القانون (١) سواء اتخذ للشرط المنصوص عليه فهي شكل التزام أو اكتفي في القانون بمجرد النص علي العواقب التي تترتب علي عدم وجود توقيع.

٣) لا تسري أحكام هذه المادة علي ما يلي: (.....)

٧٢- وتستند المادة ٧ إلي الاعتراف بوظائف التوقيع في بيئة ورقية، علي النحو المبين في الفقرة ٢٩ أعلاه.

٧٣- وبغية ضمان أن الرسالة التي يشترط توثيقها لا تجرد من القيمة القانونية لا لسبب إلا لأنها غير موقعة بأحدى الوسائل التي تتميز بها المستندات الورقية، تعتمد المادة ٧ نهجا شاملا. فهي تحدد الشروط العامة الواجب توافرها حتى تعتبر رسائل البيانات موقعة توثيقا يتسم بالمصادقية بما فيه الكفاية وحتى تكون واجبة النفاذ رغم وجود شروط التوقيع التي تشكل حاليا عقبات تعترض التجارة الإلكترونية، ركز المادة ٧ عليوظيفتين الأساسيتين للتوقيع وهما تحديد هوية محرر الوثيقة والتأكيد علي موافق محرر تلك الوثيقة علي مضمونها. وتقرر الفقرة (١) (أ) المبدأ الذي يفيد بأن الوظائف القانونية الأساسية للتوقيع يتم أدائها، في البيئة الإلكترونية، باستخدام طريقة لتحديد هوية منشئ رسالة البيانات وللتأكد علي موافقة المنشئ علي رسالة البيانات تلك.

٧٤- وترسي الفقرة (١) (ب) نهجا مرنا فيما يتعلق بمستوى الأمان الذي ينبغي أن توفره طريقة تحديد الهوية المستخدمة في الفقرة (١) (أ). وينبغي أن تكون الطريقة المستخدمة بموجب الفقرة (١) (أ) قابلة للتحويل عليها بالقدر الملائم للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق بين منشئ رسالة البيانات والمرسل إليه.

٧٥- ولدى البت فيما إذا كانت الطريقة المستخدمة بموجب الفقرة (١) (أ) طريقة مناسبة، فإن العوامل القانونية والتقنية والتجارية التي يمكن وضعها في الاعتبار تتضمن ما يلي:

(أ) مستوى التطور التقني للمعدات التي يستخدمها كل طرف من الأطراف،

(ب) طبيعة النشاط التجاري لتلك الأطراف،

(ج) التواتر الذي تحدث به المعاملات التجارية بين الأطراف.

(د) نوع المعاملة وحجمها،

(هـ) وظيفة الشروط الخاصة بالتوقيع في أية بيئة قانونية وتنظيمية معينة.

(و) نظم الاتصال،

(ز) الامتثال لإجراءات التوثيق التي يحددها الوسطاء،

(ح) النطاق المتنوع من إجراءات التوثيق الذي يتيح أي وسيط،

(ط) الامتثال للأعراف والممارسات التجارية،

(ي) وجود آليات للتغطية التأمينية إزاء الرسائل غير المأذون بها،

(ك) أهمية قيمة المعلومات الواردة في رسالة البيانات،



(ل) توافر طرائق بديلة لتحديد الهوية، وتكاليف التنفيذ،  
(م) مدى قبول طريقة تحديد الهوية أو عدم قبولها في الصناعة المعنية  
أو الميدان المعني، في الوقت الاتفاق علي التحريقة وفي الوقت الذي  
تبلغ فيه رسالة البيانات،  
(ن) أي عوامل أخرى ذات صلة (دليل تشريع قانون الأونسيترال  
النموذجي بشأن التجارة الإلكترونية، الفقرات ٥٣ و ٥٦ علي ٥٨).  
٧٦- واستنادا علي المعيار المرن المبين في المادة ٧ (١) (ب) من  
قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، تنشئ المادتان ٦ و  
٧ من القانون النموذجي الجديد آلية يمكن بها جعل التوقيعات الإلكترونية  
التي تستوفي المعايير الموضوعية لقابلية التعويل التقني عليها تنال البت  
المبكر في مفعولها القانوني. وهنا بالوقت الذي يتم فيه التأكد من الاعتراف  
بتوقيع إلكتروني باعتباره يناظر وظيفيا التوقيع الخطي، ينشئ القانون  
النموذجي نظامين متميزين. فالنظام الأول والأعم و النظام المبين في المادة  
٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية وهو يتناول أي  
"طريقة" يمكن استخدامها لاستيفاء الاشتراط القانوني الذي يقتضي التوقيع  
الخطي. أما المفعول القانوني لتلك "الطريقة" كنظير للتوقيع الخطي فيتوقف  
علي إثبات أنها جديرة بالتعويل عليها لدى جهة ثبت في الواقع، والنظام  
الثاني والأضيق هو النظام الذي ينشئه القانون النموذجي. وهو يتناول طرائق  
التوقيع الإلكتروني التي قد تعترف سلطة تابعة دولة، أو هيئة خاصة معتمدة،  
أو تعترف الأطراف نفسها، بأنها تستوفي معايير قابلية التعويل التقني المبينة  
في القانون النموذجي (انظر الوثيقة A/ CN. 9/484، الفقرة ٤٩). ومزية  
ذلك الاعتراف هي أنه يحقق اليقين لمستخدمي تقنيات التوقيع الإلكتروني تلك  
قبل أن يستخدموا تقنية التوقيع الإلكتروني تلك قبل أن يستخدموا تقنية التوقيع  
الإلكتروني فعليا.

#### هـ- قواعد سلوك أساسية للأطراف المعنية:

٧٧- لا يتناول القانون النموذجي، بأي قدر من التفصيل، قضايا المسؤولية التي يمكن أن تقع علي مختلف الأطراف المشتركة في تشغيل نظم التوقيع الإلكتروني، وهي تترك هذه القضايا للقانون المطبق غير القانون النموذجي. غير أن القانون النموذجي يضع معايير يمكن أن يجري علي أساسها تقييم سلوك تلك الأطراف، أي الموقع والطرف المعول، ومقدم خدمات التصديق.

٧٨- أما بشأن الموقع، فيضع القانون النموذجي تفاصيل للمبدأ الأساسي الذي مفاده أن الموقع ينبغي أن يمارس معقولا فيما يتعلق بأداة التوقيع الإلكتروني التي لديه. إذ ينتظر من الموقع أن يمارس حرصا معقولا لنفاذ الاستخدام غير المأذون به لأداة التوقيع تلك. ولا يضمن التوقيع الرقمي في حد ذاته أن الموقع هو الشخص الذي وقع بالفعل. وفي أفضل الحالات، يوفر التوقيع الرقمي تأكيدا بأنه يمكن أن ينسب إلي الموقع (انظر الوثيقة A/ CN. 9/484، الفقرة ٥٠). وإذا كان الموقع يعلم، أو كان ينبغي له أن يعلم، بأن أداة التوقيع تعرضت لما يثير الشبهة فينبغي له أن يخطر، دون تأخير لا مسوف له، أي شخص يمكن أن يكون من المعقول توقع تعويله علي التوقيع الإلكتروني أو تقديمه خدمات تدعم التوقيع الإلكتروني. وإذا استخدمت شهادة لدعم التوقيع الإلكتروني فينتظر أن يمارس الموقع حرصا معقولا لضمان دقة واكتمال كل التأكيدات الجوهرية المقدمة منه فيما يتصل بالشهادة.

٧٩- كما ينتظر من الطرف المعول أن يتخذ خطوات معقولة للتحقق من قابلية التعويل علي التوقيع الإلكتروني. وإذا كان التوقيع الإلكتروني مدعوما بشهادة فينبغي أن يتخذ الطرف المعول خطوات معقولة للتحقق مما أن كانت الشهادة صحيحة أم مغلفة أم ملغاة، وأن يراعي أي قيود مفروضة علي الشهادة.

٨٠- والواجب العام علي مقدم خدمات التصديق هو أن يستخدم نظماً وإجراءات وموارد بشرية جديرة بالثقة، وأن يتصرف وفقاً للتأكدات التي يقدمها المورد فيما يتعلق بسياساته وممارساته. علاوة علي ذلك، يتوقع من مقدم خدمات التصديق أن يمارس حرصاً معقولاً لضمان دقة واكتمال كل التأكيدات الجوهرية التي يقدمها فيما يتعلق بالشهادة. وينبغي لمورد خدمات التصديق أن يقدم في الشهادة المعلومات الضرورية التي تتيح للطرف المعول أن يحدد هوية مورد خدمات التصديق، كما ينبغي له أيضاً أن يبين ما يلي:

- أ) أن الموقع المحددة هويته في الشهادة كان يسيطر علي بيانات إنشاء للتوقيع في الوقت الذي صدرت فيه الشهادة،
- ب) أن بيانات إنشاء التوقيع كانت صالحة في التاريخ الذي صدرت فيه الشهادة أو قبله.

وينبغي لمقدم خدمات التصديق، ولصالح الطرف المعول، أن يقدم معلومات إضافية بشأن ما يلي:

- أ) الطريقة المستخدمة في تحديد هوية الموقع.
- ب) وجود أي قيود علي الأغراض أو القيمة التي يجوز أن تستخدم من أجلها بيانات إنشاء التوقيع أو الشهادة،
- ج) الحالة التشغيلية لبيانات إنشاء التوقيع،
- د) وجود أي قيود علي نطاق أو مدى مسئولية مقدم خدمات التصديق،
- هـ) ما أن كانت هناك وسائل متاحة للموقع لتقديم إشعار بأن بيانات إنشاء التوقيع قد تعرضت لما يثير الشبهة،
- و) ما أن كانت هناك خدمة إلغاء مقدمة في الوقت الملائم.

٨١- ويقدم القانون النموذجي قائمة مفتوحة بعوامل استرشادية لتقدير مدى ما تتميز به النظم والإجراءات والموارد البشرية التي يستخدمها مقدم خدمات التصديق من جدارة بالثقة.

و- إطار محايد لإزاء التكنولوجيات:

٨٢- بالنظر إلى سرعة الابتكار التكنولوجي، ينص القانون النموذجي على معايير للاعتراف القانوني بالتوقيعات الإلكترونية دون اعتبار للتكنولوجيا المستخدمة فيها (مثلا التوقيعات الرقمية التي تعتمد على نظم الترميز غير المتناظرة؛ وأدوات القياس الأحيائي التي تمكن من تحديد هوية الأفراد عن طريق سماتهم البينية، سواء عن طريق اليد أو شكل الوجه، أو قراءة بصمات الأصابع، أو التعرف على الصوت، أو فحص؛ (PINs) شبكية العين، إلخ)؛ ونظم الترميز المتناظرة؛ واستخدام أرقام الهوية الشخصية واستخدام إشارات الرموز كوسيلة للتحقق من رسائل البيانات عن طريق ما يسمى بطاقات "ذكية" أو أي أداة أخرى يحتفظ بها الموقع، والصيغ الرقمية للتوقيعات الخطية، وديناميات التوقيع، وطرائق أخرى، كالنقر على مربع الموافقة "OK- box". والتقنيات المختلفة المذكورة آنفا يمكن استخدامها معاً للتقليل من المخاطر في النظام المستخدم (انظر الوثيقة A/ CN. 9/484، الفقرة ٥٢).

ز- عدم التمييز ضد التوقيعات الإلكترونية الأجنبية:

٨٣- يقرر القانون النموذجي مبدأ أساسيا مفاده مكان المنشأ، في حد ذاته، لا ينبغي أن يكون بأية طريقة عاملا يحدد ما أن كان ينبغي، وإلى أي مبدئ ينبغي، الاعتراف بالشهادات أو التوقيعات الإلكترونية الأجنبية باعتبارها يمكن أن تكون سارية المفعول قانونيا في الدولة المشترعة (انظر الوثيقة A/ CN. 9/484، الفقرة ٥٣). فالبيت فيما كانت الشهادة أو التوقيع

الإلكتروني يمكن أن يكونا ساريي المفعول قانونيا، وإلى أي مدى يمكن ذلك، لا ينبغي أن يتوقف علي المكان الذي صدرت فيه الشهادة أو التوقيع الإلكتروني (انظر الوثيقة A/ CN. 9/483، الفترة ٢٧)، بل علي قابلية التعويل التقني عليها. وذلك المبدأ الأساسي موضح في المادة ١٢ (انظر أدناه، الفقرة ١٥٢-١٦٠).

خامسا: المساعدة التي تقدمها أمانة الأونيسترال:

أ- المساعدة علي صوغ التشريعات:

٨٤- في سياق أنشطة التدريب والمساعدة التي تضطلع بها أمانة الأونيسترال، تقدم المساعدة إلي الدول بتوفير المشورة التقنية لإعداد تشريعات تستند إلي قانون الأونيسترال النموذجي بشأن التوقيعات. كما تقدم المساعدة نفسها إلي الحكومات التي تنتظر في سن تشريعات تستند إلي قوانين الأونيسترال النموذجية (أي قانون الأونيسترال النموذجي للتحكيم التجاري الدولي، وقانون الأونيسترال النموذجي للتحويلات الدائنة الدولية، قانون الأونيسترال النموذجي لإشتراء السلع والإنشاءات والخدمات، وقانون الأونيسترال النموذجي بشأن التجارة الإلكترونية، وقانون الأونيسترال النموذجي بشأن الإعسار عبر الحدود)، أو الحكومات التي تنتظر في الانضمام إلي إحدى اتفاقيات القانون التجاري الدولي التي أعدتها الأونيسترال.

٨٥- ويمكن الحصول من الأمانة علي مزيد من المعلومات عن القانون النموذجي وعن سائر القوانين النموذجية والاتفاقيات التي وضعتها الأونيسترال، وذلك علي العنوان التالي:

ب- معلومات عن تفسير التشريعات المستندة إلي القانون النموذجي:

٨٦- ترحب الأمانة بالتعليقات المتصلة بالقانون النموذجي وبالدليل، وكذلك بالمعلومات المتصلة بسن التشريعات المستندة إلى القانون النموذجي. وعد اشتراع القانون النموذجي، سيدرج هذا القانون النموذجي في نظام معلومات السوابق القضائية المستندة إلى نصوص الأونسترال (CLOUT)، المستخدم لجمع وتعميم المعلومات عن السوابق القضائية المتعلقة بالاتفاقية والقوانين النموذجية المنبثقة عن أعمال الأونسترال. والفرض من هذا النظام هو تعزيز الوعي الدولي بالنصوص التشريعية التي صاغتها الأونسترال وتيسير تفسيرها وتطبيقها الموحدين. وتنتشر الأمانة باللغات الرسمية الست للأمم المتحدة، خلاصات للقرارات، وتوفر، مقابل رد تكاليف الاستساخ، القرارات التي أعدت الخلاصات على أساسها. والنظام مشروح في دليل المستعملين الذي يمكن الحصول عليه من "الأمانة في نسخة ورقية ( A/ CN. 9/ SER. C/GUIDE/1 ) وعلى صفحة موقع الأونسترال على الإنترنت المذكورة أعلاه.

## الفصل الثاني

### التعليقات علي المواد مادة فمادة العنوان

#### القانون النموذجي:

٨٧- ظل القانون النموذجي يدرك، طوال عملية إعداده، باعتباره إضافة علي قانون الأونسترال النموذجي بشأن التجارة الإلكترونية ينبغي أن تعامل علي قدم المساواة معه وأن يكون لها طابعه القانوني نفسه.

#### المادة ١- نطاق الانطباق

يطبق هذا القانون حيثما تستخدم توقيعات إلكترونية في<sup>(١)</sup> أنشطة تجارية<sup>(٢)</sup>. وهو لا يلغي أية قاعدة قانونية يكون القصد منها حماية المستهلك. تعليقات عامة:

٨٨- الغرض من المادة ١ هو تحديد نطاق تطبيق القانون النموذجي. والنهج المستخدم في القانون النموذجي هو العمل، من حيث المبدأ، علي تغطية جميع الأحوال الفعلية التي تستخدم فيها التوقيعات الإلكترونية، دون اعتبار لنقضية التوقيع الإلكتروني أو التوثيق المحددة المستخدمة. ورئي لدى إعداد القانون النموذجي أن استبعاد أي شكل من الأشكال أو أي وسيلة من الوسائط عن طريق قيد في نطاق القانون النموذجي قد يؤدي إلي صعوبات عملية

(1) تقترح اللجنة النص التالي للدول التي قد ترغب في توسيع نطاق تطبيق هذا القانون: "يطبق هذا القانون حيثما تستخدم توقيعات إلكترونية، ما عدا في الأحوال التالية: (...)"  
(2) ينبغي تفسير مصطلح "تجاري" تفسيراً واسعاً علي أنه يشمل المسائل الناشئة عن جميع العلاقات ذات الطابع التجاري، سواء أكانت تعاقدية أم غير تعاقدية، وتشمل العلاقات ذات الطابع التجاري للمعاملات التالية علي سبيل المثال لا الحصر: أية معاملة تجارية لتوريد أو تبادل السلع أو الخدمات، اتفاق التوزيع، التمثيل التجاري أو الوكالة التجارية، العملة، البيع الإيجاري، تشييد المنشآت، الخدمات الاستشارية، الأعمال الهندسية، منح الرخص، الاستثمار، التمويل، الأعمال المصرفية، التأمين، اتفاق أو امتياز الاستغلال، المشاريع المشتركة وغيرها من أشكال التعاون الصناعي أو الأعمال، نقل البضائع أو الركاب جواً أو بحراً أو بالسكك الحديدية وبالطرق البرية.

وسيتأفي مع الغرض المتمثل في توفير قواعد "محايدة إزاء الوسائط"، وكذلك "محايدة إزاء التكنولوجيات"، حياداً حقيقياً. ولدى إعداد القانون النموذجي، راعى فريق الأونسيرال العامل المعني بالتجارة الإلكترونية مبدأ الحياد التكنولوجي، وأن كل من يدرك أن "التوقعات الرقمية"، أي التوقعات الإلكترونية التي يتحصل عليه بتطبيق الترميز بواسطة زوج مفاتيح، على تكنولوجيا واسعة الانتشار بوجه خاص (انظر الوثيقة A/ CN. 9/484، الفقرة ٥٤).

#### الحاشية\*:

٨٩- يطبق القانون النموذجي على جميع أنواع الرسائل البيانات التي تمهر بتوقيع إلكتروني ذي دلالة قانونية، ولا يوجد في القانون النموذجي ما يمنع دولة مشترعة من توسيع نطاق القانون النموذجي ليشمل استخدام التوقعات الإلكترونية خارج المجال التجاري. فمثلاً في حين أن تركيز القانون النموذجي لا ينصب على العلاقات بين مستعملي التوقعات الإلكترونية والسلطات العمومية، فإن القانون النموذجي ليس مقصوداً به أن يكون قابل للتطبيق على تلك العلاقات. وتقدم الحاشية\* صيغة بديلة يمكن أن تستخدمها الدول المشترعة التي تري أن من الملائم توسيع نطاق القانون النموذجي إلى ما يتجاوز المجال التجاري.

#### الحاشية\*\*:

٩٠- رئي أن القانون النموذجي ينبغي أن يحتوي على الإشارة إلى أن تركيزه ينصب على الأنواع من الأحوال التي تصادف في الميدان التجاري وأنه عد انطلاقة من الخلفية المتمثلة في العلاقات التي تنشأ في مجال التجارة والمال. ولذلك السبب، تشير المادة ١ إلى "أنشطة تجارية"، وتقدم، في الحاشية\*\* إشارات بشأن معنى تلك العبارة. وهذه الإشارات يمكن أن تكون ذات فائدة على وجه الخصوص للبلدان التي لا يوجد فيها قانون تجاري



منفصل، وهي مصوغة، لدواعي الاتساق، علي غرار حاشية المادة ١ من قانون الأونسيترال النموذجي للتحكيم التجاري الدولي (المنقولة أيضا باعتبارها الحاشية\*\*\*\* علي المادة ١ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية). وفي بلدان معينة، لا يعتبر استخدام الحواشي في النصوص القانونية ممارسة تشريعية مقبولة، ولذلك يمكن للسلطات الوطنية المشترعة القانون النموذجي أن تتظر في إمكانية إدراج نص الحواشي في متن النص نفسه.

#### حماية المستهلكين:

٩١- توجد لدى بعض البلدان قوانين خاصة لحماية المستهلكين يمكن أن تحكم جوانب معينة من جوانب استخدام نظم المعلومات. وفيما يتعلق بقوانين المستهلكين هذه، كما كان الحال بصدد صكوك سابقة من صكوك الأونسيترال (مقل قانون الأونسيترال النموذجي للتحويلات الدائنة الدولية وقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية)، رئي أنه ينبغي أن يشار إلي أن القانون النموذجي صيغ دون عناية خاصة بالمسائل التي قد تنشأ في سياق حماية المستهلكين. وفي الوقت نفسه، رئي أنه لا يوجد سبب لاستبعاد الأحوال المتعلقة بالمستهلكين، بواسطة حكم عام، من نطاق القانون النموذجي، خاصة وأن أحكام القانون النموذجي قد يتبين أنها مفيدة جدل لحماية المستهلكين، تبعاً للتشريعات السائدة في كل دولة مشترعة علي حدة. ولذلك تعترف المادة ١ بأن أي قانون من هذا القبيل لحماية المستهلكين يمكن أن تكون له الأسبقية علي أحكام القانون النموذجي. وإذا توصل المشرعون إلي استنتاجات مختلفة بشأن ما يترتب علي القانون النموذجي من اثر مفيد في معاملات المستهلكين في أي بلد معين فيمكن لهم أن ينظروا في استبعاد المستهلكين من نطاق تطبيق النص التشريعي الذي يشترع به القانون

النموذجي. أما مسألة من يمكن اعتبارهم "مستهلكين" من الأفراد أو الهيئات فهي متروكة للقانون الواجب تطبيقه خارج نطاق القانون النموذجي.

استخدام التوقيعات الإلكترونية في المعاملات الدولية والداخلية:

٩٢- يوصي بتطبيق القانون النموذجي على أوسع نطاق ممكن. وينبغي توخي الحذر بوجه خاص من استبعاد تطبيق القانون النموذجي بواسطة حصر نطاقه في الاستعمالات الدولية للتوقيعات الإلكترونية، لأن ذلك الحصر قد يعتبر قصورا عن تحقيق أهداف القانون النموذجي تحقيقا كاملا. فضلا عن ذلك فإن الإجراءات المتنوعة المتاحة بموجب القانون النموذجي لتقييد نطاق استخدام التوقيعات الإلكترونية إذا لزم الأمر (وذلك مثلا لأغراض السياسة العامة) قد تقلل من ضرورة تقييد نطاق القانون النموذجي. واليقين القانون الذي يتوخي أن يوفره القانون النموذجي ضروري للتجارة الداخلية الدولية. ويمكن أن يؤدي التمييز بين التوقيعات الإلكترونية المستخدمة داخليا والتوقيعات الإلكترونية المستخدمة في سياق المعاملات التجارية الدولية إلى وجود نظامين يحكمان استخدام التوقيعات الإلكترونية، وبالتالي إلى إيجاد عقبات خطيرة أمام استخدام تلك التقنيات (انظر الوثيقة A/CN.9/484، الفقرة ٥٥).

الإحالات إلى وثائق الأونيسترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرتان ٢٤١ و ٢٤٢ والفقرة ٢٨٤،  
A/CN.9/493، المرفق، الفقرات ٨٨-٩٢.  
A/CN.9/484، الفقرتان ٥٤ و ٥٥،  
A/CN.9/WG.IV/WP.88، المرفق، الفقرات ٨٧-٩١،  
A/CN.9/467، الفقرات ٢٢-٢٤،  
A/CN.9/WG.IV/WP.84، الفقرة ٢٢.

## المادة ٢- التعاريف

(أ) توقيع إلكتروني: يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات.

(ب) شهادة: تعني رسالة بيانات أو سجلاً آخر يؤكدان الارتباط بين الموقع وبيانات إنشاء التوقيع.

(ج) رسالة بيانات: تعني معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر، التبادل الإلكتروني للبيانات أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي.

(د) موقع: يعني شخصاً حائزاً على بيانات إنشاء توقيع ويتصرف إما بالأصالة عن نفسه وإما بالنيابة عن الشخص الذي يمثله.

(هـ) مقدم خدمات تصديق: يعني شخصاً يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية.

(و) طرف معول: يعني شخصاً يجوز أن يتصرف استناداً على شهادة أو إلى توقيع إلكتروني.

تعريف عبارة توقيع إلكتروني:

التوقيع الإلكتروني باعتباره نظيراً وظيفياً للتوقيع الخطي.

٩٣- يقصد بمفهوم "توقيع إلكتروني" أن يشمل جميع الاستعلامات التقليدية للتوقيع الخطي لأحداث مفعول قانوني، حيث أن تعيين هوية الموقع وقرن ذلك الشخص بمحتوى المستند ليسا أكثر من الحد الأدنى المشترك للنهوج المختلفة بشأن "التوقيع" الموجودة في النظم القانونية المتباينة (أنظر الفقرتين ١١٧ و ١٢٠ أدناه). وقد سبق أن نوقشت وظائف التوقيع الخطي تلك في سياق إعداد المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. وعليه تعريف التوقيع الإلكتروني بأنه قادر علي بيان الموافقة علي المعلومات إنما يعني أساسا وضع شرط مسبق تقني للاعتراف بتكنولوجيا معينة باعتبارها قادرة علي إنشاء نظير للتوقيع الخطي. ولا يتجاهل التعريف أن التكنولوجيات التي يشار إليها عادة بعبارة "توقيعات إلكترونية" يمكن استخدامها لأغراض غير إنشاء توقيع ذي دلالة قانونية. والتعريف إنما يبين تركيز القانون النموذجي علي استخدام التوقيعات الإلكترونية كنظائر وظيفية للتوقيعات الخطية (انظر الوثيقة A/ CN. 9/483، الفقرة ٦٢). وبغية عدم إدراج أي تقييد تقني بشأن الطريقة التي يمكن للموقع استعمالها لأداء المعادل الوظيفي للتوقيع بخط اليد، أو الإحياء بذلك التقييد التقني، فضلت صيغة مرنة تشير إلي "البيانات" التي يجوز أن تستخدم" علي أي إشارة إلي الوسائل التي يستعملها الموقع الذي هو "قادر تقنيا" علي أداء تلك الوظائف.<sup>(١)</sup>

الاستعلامات الممكنة الأخرى للتوقيع الإلكتروني:

٩٤- ينبغي التمييز بين المفهوم القانوني لعبارة "توقيع" والمفهوم التقني لعبارة "توقيع إلكتروني"، التي هي مصطلح تقني يشمل ممارسات لا تتطوي بالضرورة علي إنتاج توقيعات ذات دلالة قانونية، ولدى إعداد القانون النموذجي، رئي أنه ينبغي لفت انتباه المستعملين إلي احتمال الالتباس الذي

(١) المرجع نفسه، الفقرة ٢٤٤.

يمكن أن ينشأ عن استخدام نفس الأداة التقنية لإنتاج توقيع ذي دلالة قانونية ولوظائف أخرى تتعلق بالتوثيق أو بتعيين الهوية (انظر الوثيقة A/ CN. 9/483، الفقرة ٦٢). ويمكن أن ينشأ هذا الالتباس بشأن نية الموقع بوجه خاص، إذا كان أسلوب "التوقيع الإلكتروني" ذاته مستعملاً للتعبير عن موافق الموقع علي المعلومات "الموقع عليها"، ويمكن أن يستعمل أيضاً لأداء وظائف تعيين الهوية التي ستقتصر علي ربط اسم الموقع بإرسال الرسالة دون الإشارة إلي الموافقة علي محتوياتها (انظر الفقرة ١٢٠ أتناه). وطالما استعمل التوقيع الإلكتروني للأغراض المشمولة صراحة بالقانون النموذجي (أي التعبير عن موافقة الموقع علي المعلومات الموقع عليها)، قد يحدث في الممارسة أن يكون إنشاء هذا التوقيع الإلكتروني سابقاً لاستعماله الفعلي وفي هذه الحالة، ينبغي تقدير موافقة الموقع وقت مهر الرسالة بالتوقيع الإلكتروني وليس وقت إنشاء التوقيع<sup>(١)</sup>.

#### تعريف المصطلح شهادة:

##### الحاجة إلي تعريف:

٩٥- لا يختلف معنى الكلمة "شهادة" كما هي مستخدمة في سياق أنواع معينة من التوقيعات الإلكترونية وكما هي معرفة في القانون النموذجي، اختلافاً كبيراً عن معناها العام، وهو إنها مستند يؤكد به شخص وقائع معينة، والفرق الوحيد هو أن الشهادة في شكل إلكتروني وليست في شكل ورقي (انظر الوثيقة A/ CN. 9/484، الفقرة ٥٦) ولكن بما أن المفهوم العام للكلمة "شهادة" لا يوجد في جميع النظم القانونية، أو في جميع اللغات، فقد رئي أن من المفيد إدراج تعريف لها في سياق القانون النموذجي (انظر الوثيقة A/ CN. 9/483، الفقرة ٦٥).

---

(١) المرجع نفسه، الفقرة ٢٤٥.

#### الغرض من الشهادة:

٩٦- الغرض من الشهادة هو الاعتراف بوجود صلة بين بيانات إنشاء التوقيع والموقع أو بيان وجود تلك الصلة أو تأكيد وجودها. وتنشأ الصلة عند إنتاج بيانات إنشاء التوقيع (انظر الوثيقة A/ CN. 9/483، الفقرة ٦٧).

#### بيانات إنشاء التوقيع:

٩٧- المقصود بعبارة "بيانات إنشاء التوقيع"، في سياق التوقيعات الإلكترونية التي ليست توقيعات رقمية، هو الإشارة إلى المفاتيح السرية أو الرموز أو العناصر الأخرى التي تستخدم في عملية إنشاء التوقيع الإلكتروني الناتج والشخص الموقع (انظر الوثيقة A/ CN. 9/484، الفقرة ٥٧). ففي سياق التوقيعات الإلكترونية التي تعتمد على أدوات القياس الأحيائي، مثلاً يكون العنصر الأساسي هو مؤشر القياس الأحيائي، مثل، يكون العنصر الأساسي هو مؤشر القياس الأحيائي، مثل بصمة الإصبع أو بيانات فحص الشبكية. ولا يشمل التعريف سوى العناصر الجوهرية التي ينبغي الحفاظ على سريتها لضمان نوعية عملية التوقيع، باستبعاد أي عنصر آخر يمكن الكشف عنه دون الإضرار بقابلية التعويل على التوقيع الإلكتروني الناتج، على الرغم من أن تلك العنصر يمكن أن يساهم في عملية التوقيع. ومن جهة أخرى، وفي سياق التوقيعات الرقمية التي تعتمد على الترميز غير المتناظر، فإن العنصر التشغيلي الجوهري الذي يمكن وصفه بأنه "مرتبط بالموقع" هو زوج مفاتيح الترميز. وفي حالة التوقيعات الرقمية، يكون كل من المفتاح العمومي والمفتاح الخصوصي مرتبطين بالشخص الموقع. ونظراً لأن الغرض الرئيسي من أي شهادة، في سياق التوقيعات الرقمية، هو تأكيد الصلة بين المفتاح العمومي والموقع (انظر الفقرات ٥٣-٥٦ و ٦٢ (١٠) أعلاه)، من الضروري أيضاً التصديق على أن المفتاح العمومي يرتبط بالموقع. وفي حين أن وصف "بيانات إنشاء التوقيع" هذا لا يشمل سوى المفتاح الخصوصي، فمن

المهم الإشارة، تفاديا للوقائع في الشك، إلى أنه ينبغي اعتبار أن تعريف "الشهادة" في سياق التوقيعات الرقمية، والوارد في الفقرة الفرعية (ب) من المادة ٢، يشمل تأكيد الصلة بين الموقع والمفتاح العمومي المرتبط بالموقع. ومن العناصر التي لا ينبغي أيضا أن يشملها هذا الوصف النص الذي يجري التوقيع عليه إلكترونيا وذلك على الرغم من أنه له أيضا دورا هاما في عملية إنشاء التوقيع (من خلال دالة البعثرة أو غير ذلك). وتعتبر المادة ٦ عن الفكرة التي مفادها أن بيانات إنشاء التوقيع ينبغي أن ترتبط بالموقع وليس بأي شخص آخر (انظر الوثيقة A/ CN. 9/483، الفقرة ٧٥).

#### تعريف عبارة رسالة بيانات:

٩٨- أخذ تعريف عبارة "رسالة بيانات" من المادة ٢ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، باعتباره مفهوما واسعا يشمل جميع الرسائل التي تنتج في سياق التجارة الإلكترونية، بما في ذلك التجارة المستندة إلى شبكة الويب (انظر الوثيقة A/ CN. 9/483، الفقرة ٦٩). ولا يقتصر مفهوم عبارة "رسالة بيانات" على الاتصالات، بل يقصد به أيضا أن يشمل السجلات المنتجة حاسوبيا لغرض الاتصالات. وعليه فإن مفهوم عبارة "رسالة" يشمل مفهوم عبارة "سجل".

٩٩- ويقصد بالإشارة إلى "الوسائل المشابهة" تبيان أن الغرض من القانون النموذجي ليس أن يطبق في سياق تقنيات الاتصال القائمة فحسب بل أن يستوعب أيضا التطورات التقنية المتوقعة. وهدف تعريف "رسالة البيانات" أن يشمل جميع أنواع الرسائل المنتجة أو المخزونة أو المبلغة في شكل غير ورقي أساسا. ولهذا الغرض، فإن المقصود أن تستوعب الإشارة إلى "الوسائل المشابهة" جميع وسائل إيلاخ المعلومات وتخزينها التي قد تستعمل لأداء وظائف موازية للوظائف التي تؤدي بالوسائل المذكورة في التعريف، على الرغم من أن وسائل الاتصال والإبلاغ "الإلكترونية" و "البصرية"، على سبيل

المثال، قد لا يكون مشابهة بالمعنى الدقيق للعبارة. ولأغراض القانون النموذجي، فإن كلمة "مشابهة" تعني "نظيرة وظيفيا".

١٠٠- كما يقصد من تعريف "رسالة البيانات" أيضا، أن يشمل حالة الإلغاء أو التعديل، ويفترض أن يكون لرسالة البيانات مضمون ثابت من المعلومات، ولكن يجوز أن تلغي أو تعدل برسالة بيانات أخرى (دليل تشريع قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، الفقرات ٣٠-٣٢).

تعريف المصطلح موقع شخصا:

١٠١- اتساقا مع النهج المتبع في قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، ينبغي فهم أي إشارة في القانون النموذجي الجديد إلى الكلمة "شخص" باعتبارها تشمل جميع أنواع الأشخاص أو الهيئات، سواء الأشخاص الطبيعيين أو الشركات أو الهيئات الاعتبارية الأخرى (انظر الوثيقة A/ CN. 9/483، الفقرة ٨٦).

بالنيابة عن الشخص الذي يمثل:

١٠٢- قد لا تكون المقارنة بالتوقيعات بخط اليد ملائمة دائما للاستفادة من الإمكانيات التي تتيحها التكنولوجيا العصرية. ففي بيئة ورقية، مثلا، لا يمكن للهيئات الاعتبارية أن تكون، بالمعنى الدقيق، موقعة علي الوثائق التي يصاغ نيابة عنها، لأن الأشخاص الطبيعيين هم وحدهم الذين يستطيعون إنتاج توقيعات أصلية بخط اليد. أما التوقيعات الإلكترونية فيمكن تصميمها بحيث يمكن أن تنسب إلى الشركات أو غيرها من الهيئات الاعتبارية (بما في ذلك الهيئات الحكومية وسائر الهيئات العمومية)، وقد توجد حالات تكون فيها هوية الشخص الذي يقوم بالتوقيع فعليا، عندما يكون التصرف البشري لازما، غير ذات صلة بالأغراض التي ينشأ التوقيع من أجلها (انظر الوثيقة A/ CN. 9/483، الفقرة ٨٥).



ومع ذلك ففي إطار القانون النموذجي لا يمكن فصل مفهوم المصطلح "موقع" عن الشخص الذي أنتج أو الهيئة التي أنتجت فعليا التوقيع الإلكتروني، لأن عدد من الالتزامات المحددة التي تقع علي عاتق الموقع بموجب القانون النموذجي مقترن منطقيا بالتحكم الفعلي في بيانات إنشاء التوقيع. غير أنه، لأجل تغطية الحالات التي يتصرف فيها الموقع كممثل لشخص آخر، أبقى علي عبارة "أو بالنيابة عن الشخص الذي يمثله" في تعريف الكلمة "موقع". ومسألة المدى الذي يمكن إليه يكون الشخص ملزما بتوقيع إلكتروني أنتج "نيابة عنه" هي مسألة ينبغي أن تسوي وفقا للقانون الذي يحكم، حسب الاقتضاء، العلاقة القانونية بين الموقع والشخص الذي حددت إنتاج التوقيع الإلكتروني نيابة عنه، من جهة، والطرف المعول، من جهة أخرى. فذلك المسألة، وكذلك المسائل الأخرى المتعلقة السببية، بما في ذلك مسائل الوكالة وغيرها من المسائل المتعلقة بمن يتحمل المسؤولية النهائية عن عدم امتثال الموقع لالتزاماته بموجب المادة ٨ (أي هل هو الموقع أم الشخص الذي يمثله الموقع) هي خارج نطاق القانون النموذجي (انظر الوثيقة A/ CN. 9/483، الفقرتان ٨٦ و ٨٧).

#### تعريف عبارة مقدم خدمات تصديق:

١٠٤- كحد أدنى، يتعين علي مقدم خدمات التصديق، وفقا لتعريفه لأغراض القانون النموذجي، أن يوفر خدمات التصديق، ويمكن أن يكون ذلك مع خدمات أخرى (انظر الوثيقة A/ CN. 9/483، الفقرة ١٠٠).

١٠٥- ولم يميز في القانون النموذجي بين الأحوال التي يمارس فيها مقدم خدمات التصديق خدمات التصديق باعتبار ذلك نشاطه الرئيسي أو بصفة عمل فرعي، أو عادة أو عرضا، أو مباشرة أو عبر متعاقد من الباطن. ويشمل التعريف جميع الهيئات التي تقدم خدمات التصديق في نطاق القانون النموذجي، أي "في سياق أنشطة تجارية". غير أنه، بالنظر علي

وجود ذلك القيد في نطاق انطباق القانون النموذجي، لن تكون الهيئات التي تصدر لأغراضها الداخلية وليس للأغراض التجارية داخلة في فئة "مقدمي خدمات التصديق" كما هي معرفة في المادة ٢ (انظر الوثيقة A/ CN. 9/483 ، المواد ٩٤ - ٩٩).

#### تعريف عبارة طرف معول:

١٠٦- المقصود بتعريف عبارة "طرف معول" ضمان الاتساق في تعريف الأطراف المختلفة ذات الصلة بتشغيل مخططات التوقيعات الإلكترونية بموجب القانون النموذجي (المصدر نفسه، الفقرة ١٠٧). ولأغراض ذلك التعريف، ينبغي تفسير عبارة "يتصرف" تعريفاً واسعاً بحيث لا تشمل التصرف الإيجابي وحده بل تشمل الإغفال أيضاً (A/ CN. 9/483 ، الفقرة ١٠٨).

#### الإحالات علي وثائق الأونسترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢٠٥-٢٠٧ و ٢٤٣-٢٥١، و ٢٨٤، A/CN.9/493، المرفق، الفقرات ٩٣، ١٠٦، A/CN.9/484، المرفق ٥٦ و ٥٧. A/CN.9/WG.IV/WP.88، المرفق، الفقرات ٩٢، ١٠٥، A/ CN. 9/483، الفقرات ٥٩-١٠٩، 84 و A/ CN.9/ WG. IV/ WP ، الفقرات ٢٣-٣٦، A/ CN. 9/ 465، الفقرة ٤٢، 82 و A/ CN.9/ WG. IV/ WP، الفقرات ٢٢-٣٣، A/CN.9/457، الفقرات ٢٢-٤٧، ٦٦-٦٧، ٨٩، ١٠٩،

A/CN.9/WG.IV/WP.80، الفقرات ٧-١٠،

A/CN.9/WG.IV/WP.79، الفقرة ٢١،

A/CN.9/454، الفقرة ٢٠،

A/CN.9/WG.IV/WP.76، الفقرات ١٦-٢٠،

A/CN.9/446، الفقرات ٢٧-٤٦ (مشروع المادة ١)، ٦٢-٧٠

(مشروع المادة ٤)، ١١٣-١٣١ (مشروع المادة ٨)، ١٣٢ و ١٣٣  
(مشروع المادة ٩)،

A/CN.9/WG.IV/WP.73، الفقرات ١٦-٢٧، ٣٧-٣٨، ٥٠-

٥٧، ٨٥-٦٠، A/CN.9/437، الفقرات ٢٩-٥٠ و ٩٠-١١٣ (مشاريع

المواد أ-ب-ج)، A/CN.9/WG.IV/WP.71، الفقرات ٥٢-٦٠.

### المادة ٣- المعاملة المتكافئة لتكنولوجيا التوقيع

لا يطبق أي من أحكام هذا القانون، باستثناء المادة ٥، بما يشكل استبعادا أو تقييدا أو حرمانه من مفعول قانون لأي طريقة لإنشاء توقيع إلكتروني تقي بالاشتراطات المشار إليها في الفقرة ١ من المادة ٦ أو تقي علي نحو آخر بمقتضيات القانون المطبق.

#### الحيداء إزاء التكنولوجيا:

١٠٧- تجسد المادة ٣ المبدأ الأساسي الذي مفاده أنه لا ينبغي التمييز ضد أي طريقة للتوقيع الإلكتروني، أي أن تتل جميع التكنولوجيات نفس الفرصة لاستيفاء الشروط الواردة في المادة ٦ ونتيجة ذلك، لا ينبغي أن يكون هناك اختلاف في المعاملة بين الرسائل الموقعة إلكترونيا والمستندات الورقية التي تحمل توقيعها خطيا، أو بين مختلف أنواع الرسائل الموقعة إلكترونيا، شريطة أن تستوفي الشروط الأساسية المبينة في الفقرة ١ من المادة ٦ من القانون النموذجي أو أي شرط آخر مدرج في القانون المطبق. وتلك

الشروط يمكن، مثلا، أن تقضي باستخدام تقنية توقيع مسماة علي وجه التحديد في أحوال معينة، أو قد تضع، بطريقة أخرى، معيارا قد يكون أعلي أو أدنى من المعيار الوارد في المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (والمادة ٦ من القانون النموذجي). والمقصود أن يطبق المبدأ الأساسي الخاص بعدم التمييز تطبيقا عاما، غير أنه ينبغي أن يلاحظ أن ذلك المبدأ ليس مقصودا منه أن يمس حرية التعاقد المسلم بها بموجب المادة ٥. وعليه ينبغي أن تبقى للأطراف، فيما بينها وإلى المدى الذي يسمح به القانون، حرية أن تستبعد، باتفاق بينها استخدام تقنيات توقيع إلكتروني معينة. وبالنص علي أنه "لا يطبق أي من أحكام هذا القانون.. بما يشكل استبعادا أو تقييدا أو حرمانا من مفعول قانوني لأية طريقة لإنشاء توقيع إلكتروني"، فإنما تشير المادة ٣ إلي أن الشكل الذي يتم به التوقيع الإلكتروني معين لا يمكن أن يستخدم كسبب وحيد يحرم به ذلك التوقيع من الأثر القانوني. غير أن المادة ٣ لا ينبغي أن تفسر بأنها تقرر الصحة القانونية لأية تقنية توقيع معينة أو أية معلومات موقعة إلكترونيا.

#### الإحالات إلى وثائق الأونسيترال:

- الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرتان ٢٤١ و ٢٤٢ والفقرة ٢٨٤،  
A/CN.9/493، المرفق، الفقرة ١٠٧،  
A/CN.9/WG.IV/WP.88، المرفق، الفقرة ١٠٦،  
A/CN.9/467، الفقرات ٢٥ - ٣٢،  
A/CN.9/WG.IV/WP.84، الفقرة ٣٧،  
A/CN.9/465، الفقرات ٤٣ - ٤٨،  
A/CN.9/WG.IV/WP.82، الفقرة ٣٤،

#### المادة ٤ - التفسير

١- يولي الاعتبار في تفسير هذا القانون لمصدره الدولي وللحاجة علي تسجيل توحيد تطبيقه ومراعاة حسن النية.

٢- المسائل المتعلقة بالأمور التي ينظمها هذا القانون ولا يسويها صراحة تسوي وفقا للمبادئ العامة التي يستند إليها هذا القانون.

#### المصدر:

١٠٨- المادة ٤ مستوحاة من المادة ٧ من اتفاقية الأمم المتحدة بشأن عقود البيع الدولي للبضائع، ومقتبسة من المادة ٣ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. ويقصد بها أن تقدم إرشادا يساعد هيئات التحكيم والمحاكم والسلطات الإدارية الوطنية أو المحلية علي تفسير القانون النموذجي. والمفعول المتوقع للمادة ٤ هو تقييد المدى الذي إليه لا يمكن تفسير النص الموحد، بعد إدراجه في التشريع المحلي، إلا بالرجوع إلي مفاهيم القانون المحلي.

#### الفقرة ١:

١٠٩- الغرض من الفقرة ١ هو تنبيه أي شخص قد يطلب منه تطبيق القانون النموذجي إلي أن أحكام القانون النموذجي (أو أحكام الصك الذي ينفذ القانون النموذجي)، في حين أنها تسن باعتبارها جزءا من التشريع الداخلي وبالتالي فهي دلخية في طبيعتها، ينبغي أن تفسر بالرجوع إلي منشئها الدولي، بغية كفالة الاتساق في تفسير القانون النموذجي في جميع البلدان التي تشترعه.

#### الفقرة ٢:

١١٠- من المبادئ العامة التي يستند إليها القانون النموذجي، يمكن أن يتبين أن القائمة غير الحصرية التالية قابلة للتطبيق:

(أ) التجارة الإلكترونية بين البلدان وداخلها.

(ب) إقرار صحة المعاملات التي تجري بواسطة تكنولوجيات المعلومات الجديدة.

(ج) ترويج وتشجيع استخدام التكنولوجيات المعلومات الجديدة عموماً والتوقيعات الإلكترونية خصوصاً، وذلك بطريق محايدة إزاء التكنولوجيات.

(د) تعزيز توحيد القانون.

(هـ) دعم الممارسات التجارية. وفي حين أن الغرض العام للقانون النموذجي هو تيسير استخدام التوقيعات الإلكترونية فإنه لا ينبغي أن يعتبر علي أي نحو أن القانون النموذجي يفرض استخدام التوقيعات الإلكترونية فرضاً.

الإحالات إلى وثائق الأونسترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢٥٤ و ٢٥٥ و ٢٨٤،

A/CN.9/493، المرفق، الفقرة ١٠٨-١١٠،

A/CN.9/WG.IV/WP.88، المرفق، الفقرات ١٠٧-١٠٩،

A/CN.9/467، الفقرات ٣٣-٣٥،

A/CN.9/WG.IV/WP.84، الفقرة ٣٨، ،

A/CN.9/465، الفقرتان ٤٩-٥٠،

A/CN.9/WG.IV/WP.82، الفقرة ٣٥،

#### المادة ٥- التغيير بالاتفاق

يجوز الاتفاق علي الخروج علي أحكام هذا القانون أو تغيير مفعولها، ما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضي قانون المطبق.

١١١- كان قرار الاضطلاع بإعداد القانون النموذجي مستندا إلى إدراك أن الحلول للصعوبات القانونية التي يثيرها استخدام وسائل الاتصال الحديثة تنتم في معظم الأحيان، في الممارسة العملية، في إطار العقود. ولذلك يقصد من القانون النموذجي أن يدعم مبدأ حرية الأطراف. بيد أن القانون المطبق قد يضع حدودا لتطبيق ذلك المبدأ. ولا ينبغي تفسير المادة ٥ خطأ بأنها تسمح للأطراف بالخروج على القواعد الإلزامية، مثل القواعد التي تعتمد لأسباب تتعلق بالسياسة العامة. كما لا ينبغي تفسير المادة ٥ خطأ بأنها تشجع الدول على وضع تشريع إلزامي يحد من حرية الأطراف فيما يتعلق بالتوقيعات الإلكترونية أو يدعو الدول، بطريق أخرى، على تقييد حرية الأطراف في الاتفاق فيما بينها على مسائل اشتراطات الشكل التي تنظم اتصالاتها.

١١٢- ومبدأ حرية الأطراف يطبق عموما فيما يتعلق بأحكام القانون النموذجي لأن القانون النموذج لا يحتوي على أي حكم إلزامي. ويطبق ذلك المبدأ أيضا في سياق الفقرة ١ من المادة ١٢، ولذلك لا تحد الفقرة من المادة ١٢ من حرية أطراف المعاملة التجارية في الاتفاق على استعمال الشهادات التي تنشأ من مكان معين، رغم أم محاكم الدولة المشتري أو السلطات المسؤولة عن تطبيق القانون النموذجي لا ينبغي أن تنكر أو تلغي المفاعيل القانونية لشهادة أجنبية استنادا على المكان الذي صدرت فيه الشهادة وحده (A/ CN. 9/483، الفقرة ١١٢).

اتفاق صريح أم ضمني:

١١٣- بشأن طريقة التعبير في المادة ٥ عن مبدأ حرية الأطراف، اعتراف عموما لدى إعداد القانون النموذجي بأن التغيير بالاتفاق يمكن أن يعرف عنه صراحة أو ضمنا، وقد أقيمت صياغة المادة ٥ متوافقة من المادة

٦ من اتفاقية الأمم المتحدة بشأن عقود البيع الدولي للبضائع (انظر الوثيقة A/CN.9/467، الفقرة ٣٨).

اتفاق ثنائي أم متعدد الأطراف:

١١٤- يقصد من المادة ٥ أن تطبق ليس فقط في سياق العلاقات بين مصدري رسائل البيانات والمرسل إليها تلك الرسائل بل أيضا في سياق العلاقات بالوسطاء وعليه يمكن تغيير أحكام القانون النموذجي أما باتفاقيات ثنائية أو متعددة الأطراف تبرم بين الأطراف أو بواسطة قواعد النظام التي يتفق عليها الأطراف. ونموذجيا يحصر القانون المطبق حرية الأطراف في الحقوق والالتزامات الناشئة بين الأطراف وذلك بغية تفادي أن ينطوي القانون المطبق على أي تأثير في حقوق الأطراف الثالثة والتزاماتها.

الإحالات إلى وثائق الأونيسترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢٠٨-٢٠٩-٢٥٦-٢٥٧ و ٢٨٤،

A/CN.9/493، المرفق، الفقرات ١١١-١١٤،

A/CN.9/WG.IV/WP.88، المرفق، الفقرات ١١٠-١١٣،

A/CN.9/467، الفقرات ٣٦-٤٣،

A/CN.9/WG.IV/WP.84، الفقرتان ٣٩ و ٤٠،

A/CN.9/465، الفقرات ٥١-٦١،

A/CN.9/WG.IV/WP.82، الفقرات ٣٦-٤٠،

A/CN.9/457، الفقرات ٥٣-٦٤،



## المادة ٦- الامتثال لاشتراط التوقيع

١- حيثما يشترط القانون وجود توقيع من شخص، يعد ذلك الشرط مستوفي بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني يعول عليه بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة بيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق ذي صلة.

٢- تطبق الفقرة ١ سواء أكان الشرط المشار إليه فيها في شكل التزام أو كان القانون يكتفي بالنص على نتائج تترتب على عدم وجود توقيع.

٣- يعتبر التوقيع الإلكتروني معولا عليه لغرض الوفاء بالشرط المشار إليه في الفقرة ١ إذا:

(أ) كانت بيانات إنشاء التوقيع مرتبطة، في السياق الذي تستخدم فيه، بالموقع دون أي شخص آخر.

(ب) كانت بيانات إنشاء التوقيع خاضعة، وقت التوقيع، لسيطرة الموقع دون أي شخص آخر،

(ج) كان أي تغيير في التوقيع الإلكتروني، يجري بعد حدوث التوقيع، قابلا للاكتشاف،

(د) كان المفروض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد وقت للتوقيع قابلا للاكتشاف.

٤- لا تحد الفقرة ٣ من قدرة أي شخص:

(أ) على القيام بأي طريقة أخرى بإثبات قابلية التعويل على التوقيع الإلكتروني، بغرض الوفاء بالشرط المشار إليه في الفقرة ١، أو

(ب) على تقديم دليلي على عدم قابلية التعويل على التوقيع الإلكتروني.

٥- لا تطبق أحكام هذه المادة على ما يلي: (.....)

## أهمية المادة ٦:

١١٥- المادة ٦ هي إحدى الأحكام الأساسية في القانون النموذجي. ويقصد من المادة ٦ أن تبني علي المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية وأن توفر إرشاد بشأن الكيفية التي يمكن بها استيفاء معيار الجدارة بالتعويل الوارد في الفقرة ١ (ب) من المادة ٧. وينبغي أن يوضح في الاعتبار لدى تفسير المادة ٦ أن الغرض من ذلك الحكم هو ضمان أنه، إذا كانت هناك أية نتيجة قانونية كان من شأنها أن تترتب علي استخدام التوقيع الخطي، فينبغي أن تترتب النتيجة نفسها علي التوقيع الإلكتروني الجدير بالتعويل عليه.

## الفقرات ١ و ٢ و ٥:

١١٦- تورد الفقرات ١ و ٢ و ٥ من المادة ٦ أحكاما مستمدة من الفقرات ١ (ب) و ٢ و ٣ من المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، علي التوالي. وفي تعريف عبارة "توقيع إلكتروني" في الفقرة الفرعية (أ) من المادة ٢ وردت صيغة مستوحاة من الفقرة ١ (أ) من المادة ٧ من ذلك القانون النموذجي.

## مفهوما عبارتي هوية وتعيين هوية:

١١٧- اتفق الفريق العامل علي أنه، لأغراض تعريف "التوقيع الإلكتروني" بموجب القانون النموذجي، يمكن أن تكون عبارة "تعيين هوية" أوسع نطاقا من مجرد تحديد اسم الموقع، ويشمل مفهوم الهوية أو تعيين الهوية تمييز الموقع، بالاسم أو لغيره، عن أي شخص آخر، ويمكن أن يشير المفهوم إلي خصائص هامة أخرى، مثل المنصب أو السلطة، أما مع ذكر اسم وإما دون إشارة إلي اسم. وعلي هذا الأساس، لا يلزم التمييز بين الهوية والخصائص الهامة الأخرى، كما يلزم تقييد القانون النموذجي بالأحوال التي

لا تستخدم فيها سوى شهادات الهوية التي يذكر فيها اسم الموقع (انظر الوثيقة A/ CN. 9/467، الفقرات ٥٦ - ٥٨).

**مفعول القانون النموذجي تغير مع تغير مستوى قابلية التعويل التقنية:**

١١٨- لدى إعداد القانون النموذجي، أعرب عن رأي مفاده أن المادة ٦ ينبغي أن تكون لها (أما من خلال إشارة إلى مفهوم "التوقيع الإلكتروني المعزز" وإما من خلال ذكر مباشر لمعايير لإثبات ما لطريقة توقيع معينة من قابلية تعويل تقنية غرض مزدوج هو إثبات ما يلي:

(أ) أنه ستترتب آثار قانونية علي تطبيق طرائق التوقيع الإلكترونية تلك التي سلم بجدارة التعويل عليها،

ب) من الناحية الأخرى، أنه لن تترتب تلك الآثار القانونية علي استخدام طرائق أقل جدارة بالتعويل عليها. غير أنه رئي عموماً أنه قد يلزم تمييز أدق بين طرائق التوقيع الإلكترونية المختلفة الممكنة لأن القانون النموذجي ينبغي أن يتفادي التمييز ضد أي شكل من أشكال التوقيع الإلكتروني، مهما بدا ذلك الشكل في ظروف معينة ساذجاً أو غير مأمون. ولذلك سيكون من المحتمل أن تترتب مفاعيل قانونية علي أي طريقة توقيع إلكتروني تطبق بغرض التوقيع علي رسالة بيانات بموجب الفقرة ١ (أ) من المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، شريطة أن تكون الطريقة ذات قابلية تعويل كافية في ضوء جميع الظروف، بما فيها أي اتفاق بين الطرفين بيد أنه، بموجب المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، فإن تقرير ماهية ما يشكل طريقة توقيع ذات جدارة بالتعويل عليها في ضوء الظروف لا يمكن أن يتم إلا بواسطة محكمة أو جهة أخرى تبث في الوقائع، تتدخل لإصدار حكم بأثر رجعي، وربما بعد وقت طويل من استخدام التوقيع الإلكتروني. خلافاً لذلك فإن القانون النموذجي

الجديد يتوقع أن ينشئ مزية لصالح تقنيات معينة، معترف بأنها ذات جدارة بالتعويل عليها بوجه خاص، أيا كانت الظروف التي تستخدم فيها. وهذا هو الغرض من الفقرة ٣، التي يتوقع منها أن تنشئ اليقين (أما من خلال افتراض أو من خلال قاعدة موضوعية)، في- أو قبل- الوقت الذي تستخدم فيه أية تقنية توقيع إلكتروني كهذه (مسبقا)، بأن استخدام التقنية المعترف بها سستنتج عنه مفاعيل قانونية مكافئة للآثار التي تترتب علي التوقيع الخطي. وعليه فالفقرة ٣ هي حكم ضروري لتحقيق هدف القانون النموذجي الجديد المتمثل في توفير يقين أكثر مما يوفره بالفعل الأونسيترال النموذجي بشأن التجارة الإلكترونية من يقين بشأن المفعول القانوني المتوقع من استخدام أنواع من التوقيعات الإلكترونية ذات الجدارة بالتعويل عليها بوجه خاص (انظر الوثيقة A/ CN. 9/465، الفقرة ٦٤).

افتراض أم قاعدة موضوعية:

١١٩- من أجل توفير اليقين بشأن المفعول القانوني المترتب علي استخدام التوقيع الإلكتروني، حسب تعريفه الوارد في المادة ٢، تقرر الفقرة ٣ صراحة المفاعيل القانونية التي تترتب علي اجتماع خصائص تقنية معينة للتوقيع الإلكتروني (انظر الوثيقة A/ CN. 9/484، الفقرة ٥٨). أما بشأن الكيفية التي يمكن أن تقرر بها تلك المفاعيل القانونية، فينبغي أن تكون للدولة المشترعة، رهنا بقانون الإجراءات المدنية والتجارية فيهما حرية أن تضع افتراضا بوجود ارتباط بين خصائص تقنية والمفعول القانوني للتوقيع أو تؤكد وجود ذلك الارتباط تأكيدا مباشرا (انظر الوثيقة A/ CN. 9/467، الفقرتين ٧١ و ٦٢).

## نية الموقع:

١٢٠- يتبقى سؤال عما أن كان ينبغي أن يترتب أي مفعول قانوني علي استخدام تقنيات التوقيعات الإلكترونية التي قد يستخدمها الموقع دون أن تكون لديها أية نية واضحة للالتزام القانوني بالموافق علي المعلومات التي يجري التوقيع عليها إلكترونيا. وفي أي طرف كهذا، لا تستوفي الوظيفة الثانية المبينة في الفقرة ١ (أ) من المادة ٧ من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، لأنه لا توجد "نية لإبداء أية موافقة علي المعلومات الواردة في رسالة البيانات". والنهج المتبع في القانون النموذجي هو أن المفاعيل القانونية المترتبة علي استخدام التوقيع الخطي ينبغي أن تتكرر في البيئة الإلكترونية وعليه فينبغي أن يفترض أن الموقع، بقيامه بتدليل معلومات معينة بتوقيع (سواء أكان خطيا أو إلكترونيا)، قد وافق علي ربط هويته بتلك المعلومات. والبت في ما أن كان ينبغي أن تترتب علي ذلك الربط مفاعيل قانونية (تعاقدية أو غير تعاقدية) ستوقف علي طبيعة المعلومات التي توقع، وعلي أية ظروف أخرى، تقيم وفقا للقانون المطبق خارج نطاق القانون النموذجي. وفي ذلك السباق، لا يقصد من القانون النموذجي أن يتدخل في القانون العام للعقود أو الالتزامات (انظر الوثيقة A/ CN. 9/465، الفقرة ٦٥).

## معايير قابلية التعويل التقنية:

١٢١- يقصد من الفقرات الفرعية (أ) إلي (د) من الفقرة ٣ التعبير عن معايير موضوعية قابلية التعويل التقنية علي التوقيعات الإلكترونية. وتركز الفقرة الفرعية (أ) علي الخصائص الموضوعية لبيانات إنشاء التوقيع، التي يجب أن تكون "مرتبطة ... بالموقع دون أي شخص آخر". ومن الجهة التقنية، يمكن أن تكون بيانات إنشاء التوقيع "مرتبة" بالموقع ارتباطا فريدا دون أن تكون هي "فريدة" في حد ذاتها. والارتباط بين البيانات المستخدمة لإنشاء التوقيع بين الموقع هو العنصر الرئيسي (انظر الوثيقة A/ CN.

9/467، الفقرة ٦٣). وفي حين أن مستعملين مختلفين يمكن أن يشتركوا في استعمال بيانات معينة لإنشاء التوقيعات الإلكترونية، وذلك مثلا إذا كان عدة موظفين يشتركون في استعمال بيانات لإنشاء التوقيع تملكها إحدى المؤسسات، فإن تلك البيانات يجب أن تكون قادرة علي تحديد هوية مستعمل واحد تحديدا لا ليس فيه في سياق كل توقيع إلكتروني علي حدة.

انفراد الموقع بالسيطرة علي بيانات إنشاء التوقيع:

١٢٢- تتناول الفقرة الفرعية (ب) الظروف التي تستخدم فيها بيانات إنشاء التوقيع. ويجب أن تكون بيانات إنشاء التوقيع، في وقت استعمالها، تحت سيطرة الموقع وحده. وفيما يتعلق بمفهوم سيطرة الموقع وحده، ينشأ سؤال عما أن كان الموقع سيحتفظ بقدرة علي الإنن لشخص آخر باستعمال بيانات التوقيع نيابة عنه. ويمكن أن ينشأ هذا الحال إذا كانت بيانات التوقيع في سياق المؤسسات حيث تكون المؤسسة هي الموقع ولكنها تحتاج إلي أن يكون عدد من الأشخاص قادرين علي التوقيع نيابة عنها (انظر الوثيقة A/ CN. 9/467، الفقرة ٦٦). وهناك مثال آخر في التطبيقات العملية، وهو أن تكون بيانات إنشاء التوقيعات موجودة في شبكة ويستطيع عدد من الناس استعمالها. وفي ذلك الحال، يفترض أن تكون الشبكة مرتبطة بكيان معين هو الموقع، وهو يحتفظ بالسيطرة علي بيانات إنشاء التوقيعات. أما إذا كان الأمر علي خلاف ذلك، وكانت بيانات إنشاء التوقيعات متاحة علي نطاق واسع، فلا ينبغي أن يتناولها القانون النموذجي (انظر الوثيقة A/ CN. 9/467، الفقرة ٦٧). وعندما يكون هناك مفتاح واحد يشغله أكثر من شخص واحد في سياق "مفتاح مشطور" أو مخطط آخر بشأن "سير متشارك فيه، تعني الإشارة إلي "الموقع" إشارة إلي أولئك الأشخاص معا (انظر الوثيقة A/ CN 9/483، الفقرة ١٥٢).

#### الوكالة:

١٢٣- تقضي الفقرتان الفرعيتان (أ) و (ب) مجتمعتين إلى ضمان أن يكون استخدام بيانات إنشاء التوقيع في أي وقت معين، وهو أساسا وقت التوقيع، بمستطاع شخص واحد فقط وليس بمستطاع أي شخص آخر أيضا (انظر الفقرة ١٠٣ أعلاه)، أما مسألة الوكالة، أو استخدام بيانات إنشاء التوقيع استخداما ماذونا به، فيتناولها تعريف المصطلح "موقع"، (انظر الوثيقة A/ CN. 9/467، الفقرة ٦٨).

#### السلامة:

١٢٤- تتناول الفقرتان الفرعيتان (ج) و (د) مسائل سلامة التوقيع الإلكتروني وسلامة المعلومات التي يوقع عليها إلكترونيا، وكان بالإمكان دمج الحكمين معا بغية التشديد على فكرة أنه، إذا مهر مستند بتوقيع، تكون سلامة المستند وسلامة التوقيع مرتبطتين ارتباطا يبلغ من الوثاقة أن يصعب تصور أحدهما دون الآخر. غير أنه تقرر أنه يتبع القانون النموذجي التمييز المقرر في قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية بين المادتين ٧ و ٨. فعلى الرغم من أن بعض التكنولوجيات توفر كلا من التوثيق (المادة من القانون النموذجي بشأن التجارة الإلكترونية) والسلامة (المادة ٨ من القانون النموذجي بشأن التجارة الإلكترونية) فإن ذلك المفهومين يمكن أن يعتبرا مفهومين قانونيين متميزين، وأن يعاملا على ذلك الأساس. وبما أن التوقيع الخطي لا يوفر ضمانا لسلامة المستند الذي ي مهر به ولا ضمانا بأن أي تغيير يجري في المستند سيتسنى اكتشافه، فإن نهج التناظر الوظيفي يقتضي عدم تناول ذلك المفهومين في حكم واحد. والغرض من الفقرة ٣ (ج) هو وضع معيار يتعين استيفاؤه من أجل إثبات أن أي طريقة توقيع إلكتروني معينة هي طريقة جديدة بالتعويل عليها بما يكفي لاستيفاء اشتراط قانوني بأن يكون هناك توقيع. ويمكن استيفاء ذلك الاشتراط

القانوني دون حاجة إلى إثبات سلامة المستند في مجمله ((انظر الوثيقة A/ CN. 9/467، الفقرة ٧٢ - ٨٠)).

١٢٥- ويقصد من الفقرة الفرعية (د) أساساً أن تستخدم في البلدان التي تكون فيها القواعد القانونية الراهنة النازمة لاستخدام التوقيعات الخطية غير قابلة لاستيعاب تمييز بين سلامة التوقيع وسلامة المعلومات التي يجري التوقيع عليها. وفي البلدان الأخرى، يمكن أن تؤدي الفقرة الفرعية (د) إلى إنشاء توقيع أكثر جدارة بالتعويل عليه من التوقيع الخطي، وبذلك تتعدي مفهوم النظير الوظيفي للتوقيع. وفي ولايات قضائية معينة، يمكن أن يكون اثر الفقرة الفرعية (د) هو إنشاء نظير وظيفي للمستند الأصلي (انظر الوثيقة A/ CN. 9/484، الفقرة ٦٢).

التوقيع الإلكتروني على جزء من الرسالة:

١٢٦- تتضمن الفقرة الفرعية (د) تعبيراً عن الارتباط الضروري بين التوقيع والمعلومات التي يجري التوقيع عليها، وذلك لتفادي الإيحاء بأن التوقيع الإلكتروني لا يمكن أن يطبق إلا على كامل محتويات رسالة البيانات. والواقع أن المعلومات التي يوقع عليها ستكون، في كثير من الحالات، جزءاً فقط من المعلومات الواردة في رسالة البيانات، فمثلاً يمكن أن يكون التوقيع الإلكتروني غير معلق إلا بمعلومات مرفقة مع الرسالة لأغراض البث. التغيير بالاتفاق:

١٢٧- ليس مقصوداً من الفقرة (٣) أن تفيد تطبيق المادة ٥ أو أن تفيد تطبيق أي قانون مطبق يعترف بحرية الأطراف في أن تدرج في أي اتفاق ذي صلة حكماً مفاده أن تقنية توقيع معينة ستعامل فيما بينها باعتبارها نظيراً جديراً بالتعويل عليه للتوقيع الخطي.



١٢٨- ويقصد من الفقرة ٤ (أ) أن نهين أساساً قانونياً للممارسة التجارية التي في إطارها تنظم تجارية عديدة، بواسطة عقد، علاقتها فيما يتصل باستعمال التوقيعات الإلكترونية (انظر الوثيقة A/ CN. 2/484، الفقرة ٦٣). إمكانية استنباط أدلة على عدم قابلية التعويل على التوقيع الإلكتروني: ١٢٩- يقصد من الفقرة ٤ (ب) أن توضح أن القانون النموذجي لا يحد من أي إمكانية قد توجد للطعن في الافتراض المتوخي في الفقرة ٣ (انظر الوثيقة A/ CN. 9/484، الفقرة ٦٣).

#### الاستثناءات من نطاق المادة ٦:

١٣٠- المبدأ المجسد في الفقرة ٥ هو أنه يجوز للدولة المشترعة أن تستثني من تطبيق المادة ٧ أحوالاً معينة تحدد في القانون الذي يشترع به القانون النموذجي. وقد ترغب الدولة المشترعة في أن تستثني على وجه التحديد أنواعاً معينة من الأحوال، تتوقف، على الخصوص، على الغرض الذي من أجله وضع اشتراط شكلي للتوقيع الخطي، ويمكن، مثلاً، النظر في استثناء معين في سياق الشكليات المشترطة عملاً بالالتزامات التعاهدية الدولية للدولة المشترعة، وفي أنواع أخرى من الأحوال والمجالات القانونية التي ليس من صلاحيات الدولة المشترعة أن تغيرها بواسطة قانون.

١٣١- وقد أدرجت الفقرة ٥ بهدف تعزيز مقبولية القانون النموذجي، وتسلم الفقرة بأن مسألة النص على الاستثناءات ينبغي أن تترك للدولة المشترعة، ولهذا نهج من شأنه أن يراعي الاختلافات في الظروف الوطنية بطريقة أفضل. غير أنه ينبغي أن يلاحظ أن أهداف القانون النموذجي لن يتحقق إذا استخدمت الفقرة ٥ لوضع استثناءات شاملة، وينبغي اجتناب الفرصة التي تنتجها الفقرة ٥ في ذلك الصدد. فالاستثناءات العديدة من نطاق المادة ٥ من شأنها أن تضع عقبات لا لزوم لها أمام تطور التوقيعات

الإلكترونية، لأن المبادئ والنهج التي يحتوي عليها القانون النموذجي هي مبادئ ونهج أساسية يتوقع أن تطبق تطبيقاً عاماً (انظر الوثيقة A/ CN. 9/484، الفقرة ٦٣).

الإحالات على وثائق الأونسترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢٥٨، و ٢٥٩، و ٢٨٤،  
A/CN.9/493، المرفق، الفقرات ١١٥ - ١٣١  
A/CN.9/484، الفقرات ٥٨ - ٦٣،  
A/CN.9/WG.IV/WP.88، المرفق، الفقرات ١١٤ - ١٢٦،  
A/CN.9/467، الفقرات ٤٤ - ٨٧  
A/CN.9/WG.IV/WP.84، الفقرتان ٤١ - ٤٧،  
A/CN.9/465، الفقرات ٦٢ - ٨٢،  
A/CN.9/WG.IV/WP.82، الفقرات ٤٢ - ٤٤،  
A/CN.9/457، الفقرات ٤٨، ٥٢،  
A/CN.9/WG.IV/WP.80، الفقرة ١١ و ١٢،

#### المادة ٧ - الوفاء بالمادة ٦

- ١- يجوز لـ (أي شخص أو جهاز أو سلطة تعنيهم الدولة المشترعة جهة مختصة، سواء أكانت عامة أو خاصة) تحديد التوقيعات الإلكترونية التي تفي بأحكام المادة ٦ من هذا القانون.
- ٢- تعين أن يكون أي تحديد يتم بمقتضى الفقرة ١ متسقاً مع المعايير الدولية المعترف بها.

٣- ليس في هذه المادة ما يخل بسريان مفعول قواعد القانون الدولي الخاص.

#### التحديد المسبق لوضعية التوقيع الإلكتروني:

١٣٢- تبين المادة ٧ الدور الذي تؤديه الدولة المشترعة في إنشاء أي كيان يؤكد صحة استعمال التوقيعات الإلكترونية، أو يشهد بنوعيتها علي نحو آخر، أو الاعتراف بذلك الكيان. وتستند المادة ٧، مثلها المادة ٦، إلي فكرة أن ما يلزم لتيسير تطوير التجارة الإلكترونية هو توفر عنصري اليقين والقابلية للتنبؤ عند قيام الأطراف التجاريين باستخدام تقنيات التوقيع الإلكتروني، وليس عندما يوجد نزاع أمام المحكمة وحيثما تكون تسمية توقيع معينة قادرة علي الوفاء باشتراطات وجود درجة عالية من قابلية التعويل والأمن، ينبغي أن تكون هناك وسيلة لتقييم الجوانب التقنية لقابلية التعويل والأمن ولمنح تقنية التوقيع شكلا من أشكال الاعتراف.

#### الغرض من المادة ٧:

١٣٣- الغرض من المادة ٧ هو توضيح أنه يجوز للدولة المشترعة أن تسمي هيئة أو سلطة تكون لها صلاحية إصدار قرارات بشأن ماهية التكنولوجيات المحددة التي يمكن أن تطبق عليها القاعدة المقررة بموجب المادة ٦. وليست المادة ٧ حكما تخويليا يمكن، أو ينبغي، بالضرورة أن تسترعه الدول في شكله الراهن. غير أن المقصود منها هو أن توجه رسالة واضحة فحواها أن اليقين والقابلية للتنبؤ يمكن تحقيقها بتحديد ماهية تقنيات التوقيع الإلكتروني التي نفي بمعيار قابلية التعويل الوارد في المادة ٦، شريطة أن يجري ذلك التحديد وفقا للمعايير الدولية. ولا ينبغي تفسير المادة ٧ بطريق تقرر آثارا قانونية إلزامية لاستخدام أنواع معينة من تقنيات التوقيع، أو تحصر استخدام التكنولوجيات في التقنيات التي يقرر أنها نفي

بمقتضيات قابلية التعويل الواردة في المادة ٦. فينبغي أن تكون للأطراف، مثلاً، حرية استخدام تقنيات لم يقرر أنها تقي بمقتضيات المادة ٦، إذا كان ذلك ما اتفقوا عليه. وينبغي أن تكون لهم أيضاً حرية أن يبرهنوا، أمام محكمة أو هيئة تحكيم، على أن طريقة التوقيع التي اختاروا استعمالها تقي فعلاً بمقتضيات المادة ٦، حتى وأن لم تكن تلك التقنيات موضوع قرار سابق بذلك.

#### الفقرة ١:

١٣٤- توضح الفقرة ١ أن أي كيان يجوز له أن يقرر صحة استخدام التوقيعات الإلكترونية، أو يشهد بطريقة أخرى على نوعيتها، لن يتعين أن ينشأ بصفة سلطة تابعة للدولة، ولا ينبغي أن تفسر الفقرة ١ بأنها توصي الدولة بالطريقة الوحيدة لتحقيق الاعتراف بتكنولوجيات التوقيع، بل بأنها تشير على القيود التي ينبغي أن تنطبق إذا رغبت الدولة في اعتماد ذلك النهج.

#### الفقرة ٢:

١٣٥- فيما يتعلق بالفقرة ٢، لا ينبغي حصر مفهوم "المعيار" في المعايير التي تضعها، مثلاً، المنظمة الدولية لتوحيد المقاييس (إفيسو) أو فرقة العمل المعنية بهندسة الإنترنت (IETF)، أو في معايير تقنية أخرى. وينبغي تفسير عبارة "معيار" بمعنى واسع، يشمل الممارسات الصناعية والأعراف التجارية، والمعايير الطوعية (كذلك التي ورد وصفها في الفقرة ٦٩ أعلاه)، والنصوص المنبثقة من منظمات دولية مثل غرفة التجارة الدولية، وهيئات الاعتماد الإقليمية التي تعمل تحت رعاية الإيسو (انظر الوثيقة A/ CN. 484/9، الفقرة ٦٦)، وكونسورتيوم شبكة الويب العالمية (W3C)، والهيئات

الإقليمية لتوحيد المعايير<sup>(١)</sup> ، وكذلك أعمال الأونسيترال نفسها (بما فيها هذا القانون النموذجي وقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية). ولا ينبغي أن تحول إمكانية عدم وجود معايير ملائمة دون قيام الأشخاص المختصين أو السلطات المختصة بعملية البت المشار إليها في الفقرة ١. وبشأن الإشارة إلى المعايير "المعترف بها"، يمكن أن يطرح سؤال عن ماهية ما يشكل "اعترافاً" وما هي الجهة المطلوب منها ذلك الاعتراف (انظر الوثيقة A/ CN. 9/465، الفقرة ٩٤). وهذا السؤال منقش أيضاً في إطار المادة ١٢ (انظر الفقرة ١٥٩ أدناه).

### الفقرة ٣:

١٣٦- المقصود من الفقرة ٣ هو أن توضح تماماً أن الغرض من المادة ٧ ليس التدخل في الأعمال العادية لقواعد القانون الدولي الخاص (انظر A/ CN. 9/467، الفقرة ٩٤). ولو لم يكن هذا الحكم موجوداً، لأمكن تفسير مشروع المادة ٧ خطأ بأنه يشجع الدول المشترعة على التمييز ضد التوقيعات الإلكترونية الأجنبية استناداً إلى عدم الامتثال للقواعد التي يضعها الشخص المختص أو السلطة المختصة بموجب الفقرة ١.

### الإحالات على وثائق الأونسيترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢١٠-٢١١، و ٢٦٠-٢٦١ و ٢٨٤  
A/CN.9/493، المرفق، الفقرات ١٣٢-١٣٦،  
A/CN.9/484، الفقرات ٦٤-٦٦،  
A/CN.9/WG.IV/WP.88، المرفق، الفقرات ١٢٧-١٣١  
A/CN.9/467، الفقرات ٩٠-٩٥،

(١) المرجع نفسه، الفقرات ٢٧٥-٢٧٧.

#### المادة ٨ - سلوك الموقع

١- حيثما يمكن استخدام بيانات إنشاء التوقيع لإنشاء توقيع يكون له مفعول قانوني، يتعين علي كل موقع:

(أ) أن يمارس عناية معقولة لاجتناب استخدام بيانات إنشاء توقيع استخدامه غير مأذون به،

(ب) أن يستعمل، دون تأخير لا مسوغ له، الوسائل التي يتيحها له مقدم خدمات التصديق عملاً بالفقرة ٩ من هذا القانون، أو أن يبذل جهوداً معقولة أخرى، لإشعار أي شخص يجوز للموقع أن يتوقع منه علي وجه معقول أن يعول علي التوقيع الإلكتروني أو أن يقدم خدمات تأييد للتوقيع الإلكتروني، وذلك في حالة:

(١) معرفة الموقع بأن بيانات إنشاء التوقيع تعرضت لما يثير الشبهة، أو

(٢) كون الظروف المعروفة لدى الموقع تؤدي إلي احتمال كبير بأن بيانات إنشاء التوقيع ربما تكون قد تعرضت لما يثير الشبهة،

(ج) أن يمارس، في حال استخدام شهادة لتأييد التوقيع الإلكتروني، عناية معقولة لضمان دقة واكتمال كل ما يقدمه الموقع من تأكيدات جوهرية ذات صلة بالشهادة طيلة سريانها، أو التي يتوخي إدراجها في الشهادة.

٢- يتحمل الموقع العواقب القانونية المترتبة علي تخلفه عن الوفاء  
باشتراطات الفقرة ١.

#### العنوان:

١٣٧- كان المعتزم في البداية أن تحتوي المادة ٨ (والمادتان ٩ و ١١) علي قواعد بشأن التزامات ومسئوليات مختلف الأطراف المعنية (الموقع والطرف المعول ومقدم خدمات التصديق). غير أن التغيرات السريعة المتعلقة بالجوانب التقنية والتجارية للتجارة الإلكترونية، وكذلك الدول الذي يؤديه التنظيم الذاتي حالياً في مضمار التجارة الإلكترونية في بلدان معينة، كل ذلك جعل من الصعب تحقيق آراء بشأن محتويات تلك القواعد. وقد صيغت هذه المواد بحيث تحتوي علي "قواعد سلوك" مصغرة لمختلف الأطراف. وكما هو مبين في سياق المادة ٩ بشأن مقدمي خدمات التصديق (انظر الفقرة ١٤٤ أناه)، لا يشترط القانون النموذجي علي الموقع درجة من العناية أو الجدارة بالنفقة ليست لها علاقة معقولة بالأغراض التي يستخدم من أجلها التوقيع الإلكتروني أو الشهادة (انظر الوثيقة A/ CN. 9/484، الفقرة ٦٧). ولذلك يفضل القانون النموذجي حلاً يربط الالتزامات الواردة في المادتين ٨ و ٩ كلتيهما بإنتاج توقيعات إلكترونية ذات مفعول قانوني (انظر الوثيقة A/ CN. 9/483، الفقرة ١١٧). ومبدأ مسؤولية الموقع عن عدم الامتثال للفقرة ١ منصوص عليه في الفقرة ٢، أما البت في مدى تلك المسؤولية المترتبة علي عدم الامتثال لقواعد السلوك تلك فهو متروك للقانون خارج نطاق القانون النموذجي (انظر الفقرة ١٤١ أناه).

#### الفقرة ١:

١٣٨- الفقرتان الفرعيتان (أ) و (ب) تطبقان عموماً علي جميع التوقيعات الإلكترونية، بينما لا تطبق الفقرة الفرعية (ج) علي التوقيعات

الإلكترونية المدعون بشهادات وعلي وجه الخصوص فإن الالتزام الوارد في الفقرة ١ (أ) بممارسة عناية معقولة لاجتتاب استخدام غير مأذون به هو التزام أساسي يرد عموماً، مثلاً، في الاتفاقات المتعلقة باستخدام بطاقات الائتمان. وبموجب السياسة المتبعة في الفقرة ١، ينبغي أن يطبق مثل ذلك الالتزام أيضاً علي أية بيانات إنشاء توقيع إلكتروني يمكن استخدامها لأغراض التعبير عن نية ذات دلالة قانونية. غير أن الحكم الخاص بالتغيير بالاتفاق، الوارد في المادة ٥، يسمح بتغيير المعايير المبينة في المادة ٨ في المجالات التي يري أنه غير مناسبة فيها، أو إنها تؤدي إلى نتائج غير مقصودة. وهناك حاجة، عند تفسير مفهوم "العناية المعقولة"، إلى أخذ الممارسات ذات الصلة في الحسبان، إن وجدت. كما ينبغي تفسير "العناية المعقولة" في إطار القانون النموذجي مع إيلاء الاعتبار الواجب لمصدرها الدولي، مثلما ومذكور في المادة ٤<sup>(١)</sup>.

١٣٩- وتنشئ الفقرة ١ (ب) اشتراطاً مرناً يقضي ببذل "جهود معقولة" لإشعار أي شخص يمكن أن يتوقع منه أن يعول علي التوقيع الإلكتروني في الحالات التي يبدو فيها أن التوقيع الإلكتروني قد تعرض لما يثير الشبهة. فنظراً لأنه قد يكون من المستحيل علي الموقع أن تتبع كل شخص قد يعول علي التوقيع الإلكتروني، رئي أن تحميل الموقع التزام تحقيق النتيجة المتمثلة في إشعار كل شخص يمكن تصور أنه يعول علي التوقيع و أمر يشكل عبئاً مفرداً. وينبغي تفسير مفهوم "الجهود المعقولة" علي ضوء المبدأ العام لحسن النية المعبر عنه في الفقرة ١ من المادة ٤<sup>(٢)</sup>. وتجسد الإشارة إلى "الوسائل التي يتيحها له مقدم خدمات التصديق"، حالات عملية معينة يضع فيها مقدم خدمات التصديق وسائل رهن تصرف الموقع، وذلك مثلاً في سياق

(١) المرجع نفسه، الفقرة ٢١٤.

(٢) المرجع نفسه، الفقرة ٢١٦.



الإجراءات المعتزم تطبيقها عندما يبدو أن التوقيع الإلكتروني قد تعرض لما يثير الشبهة. وهذه الإجراءات لا يجوز عموماً للموقع تغييرها. والأثر المترتب على هذه الإشارة يتمثل في تزويد الموقع بحكم "ملاذ آمن" يمكنه من البرهنة على أنه كان يقطاً بالقدر الكافي في محالة إشعار الأطراف المعولة المحتملة إذا اتبع الموقع الوسائل الموضوعية ف تصرفه<sup>(١)</sup>. وفيما يتعلق بهذه الأطراف المعولة المحتملة، تشير الفقرة ١ (ب) على مفهوم "أي شخص يجوز للموقع أن يتوقع منه على نحو معقول أن يعول على التوقيع الإلكتروني أو أن يقدم خدمات تأييداً للتوقيع الإلكتروني". ورهنا بالتكنولوجيا المستخدمة، فليّن ذلك "الطرف المعول" يمكن أن يكون ليس شخصاً يسعى على التعويل على توقيع فقط، بل شخصاً مثل مقدم خدمات تصديق أو مقدم خدمات إلغاء شهادات أو أي طرف معني آخر أيضاً.

١٤٠- وتطبق الفقرة ١ (ج) إذا استخدمت شهادة لدعم بيانات إنشاء التوقيع والمقصود أن تفسر عبارة "فترة سريان الشهادة" تفسيراً واسعاً باعتبارها تشمل المدة التي تبدأ بتقديم طلب الحصول على الشهادة أو إنشاء الشهادة وتنتهي بانتهاء فترة سريان الشهادة أو إلغائها.

#### الفقرة ٢:

١٤١- فيما يتعلق بالنتائج التي يمكن أن تترتب على عدم امتثال الموقع للاشتراطات المبينة في الفقرة ١، لا تنص الفقرة ٢ على نتائج المسؤولية ولا على حدودها، وكلا الأمرين متروك للقانون الوطني. غير أن الفقرة ٢، وأن كانت تترك نتائج المسؤولية للقانون الوطني، توجه إشارة واضحة إلى الدول المشتركة مفادها أنه ينبغي أن تترتب مسؤولية على التخلف عن استيفاء الالتزامات في الفقرة ١. وتستند الفقرة ٢ إلى الاستنتاج الذي تم التوصل إليه

(١) المرجع نفسه، الفقرة ٢١٧.

لدى إعداد القانون النموذجي، ومفاده أنه قد يكون من الصعب تحقيق توافق آراء في شكل قاعدة موحدة حول ماهية النتائج التي يمكن أن تترتب على مسئولية الموقع. ورهنا بالسباق الذي يستعمل فيه التوقيع الإلكتروني، يمكن أن تمتد تلك النتائج، بموجب القوانين الحالية، من التزام الموقع بمحتويات الرسالة على المسئولية عن دفع تعويض عن الأضرار، ولن تشمل النتائج المحتملة الأخرى بالضرورة المسئولية، لكنها يمكن أن تشمل مثلاً الحيلولة دون إنكار الطرف المخل المفعول الإلزامي للتوقيع الإلكتروني. وبغير شمل هذه النتائج الإضافية، وكذلك من أجل تجنب إحداث انطباع خاطئ بأن المقصود بالقانون النموذجي هو أن ينشئ مبدأ مسئولية صارمة، لم يرد ذكر مفهوم المسئولية ذكراً صريحاً في الفقرة ٢. وتبعاً لذلك، تكتفي الفقرة ٢ بإثبات مبدأ أن الموقع ينبغي أن يتحمل النتائج القانونية المترتبة على عدم الوفاء باشتراطات الفقرة ١، وتترك للقانون المطبق خارج إطار القانون النموذجي، في كل دولة مشترعة، تناول النتائج القانونية التي ستترتب على عدم الوفاء بتلك الاشتراطات<sup>(١)</sup>.

#### الإحالات على وثائق الأونيسترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم

١٧ (A/56/17) الفقرات ٢١٢ و ٢٢٢، و ٢٦٢ و ٢٦٣ و ٢٨٤

A/CN.9/493، المرفق، الفقرات ١٣٧-١٤١،

A/CN.9/484، الفقرات ٦٧-٦٩،

A/CN.9/WG.IV/WP.88، المرفق، الفقرات ١٣٢-١٣٦،

A/CN.9/467، الفقرات ٩٦-١٠٤،

A/CN.9/WG.IV/WP.84، الفقرات ٥٢ و ٥٣،

(١) المرجع نفسه، الفقرات ٢١٩-٢٢١

#### المادة ٩- سلوك مقدم خدمات التصديق

١- حينما يوفر مقدم التصديق خدمات لتأييد توقيع إلكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعاً، يتعين علي مقدم خدمات التصديق المشار إليه:

(أ) أن يتصرف وفقاً للتأكدات التي يقدمها بخصوص سياساته وممارساته،

(ب) أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مدرجة في الشهادة،

(ج) أن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتتمكن الطرف المعول من التأكد، من الشهادة مما يلي:

(١) هوية مقدم خدمات التصديق،

(٢) أن الموقع المعنية هويته في الشهادة كان يسيطر علي بيانات إنشاء التوقيع في الوقت الذي أصدرت فيه الشهادة،

(٣) أن بيانات إنشاء التوقيع كانت صحيحة في الوقت الذي أصدرت فيه الشهادة أو قبله،

(د) أن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتتمكن الطرف المعول من التأكد، عند الاقتضاء، من الشهادة أو من سواها، مما يلي:

- (١) الطريقة المستخدمة في تعيين هوية الموقع،  
(٢) وجود أي قيد على الغرض أو القيمة التي يجوز أن تستخدم من أجلها بيانات إنشاء التوقيع أو أن تستخدم من أجلها الشهادة،  
(٣) أن بيانات إنشاء التوقيع صحيحة ولم تتعرض لها يثير الشبهة،  
(٤) وجود أي قيد على نطاق أو مدى المسؤولية التي اشترطها مقدم خدمات التصديق.
- (٥) ما إذا كانت هناك وسائل متاحة للموقع لتقديم إشعار عملاً بالفقرة ١ (ب) بالمادة ٨ من هذا القانون،  
(٦) ما إذا كانت تتاح خدمة إلغاء ناجزة،  
(هـ) أن يوفر، حيثما تقدم الخدمات بمقتضى الفقرة الفرعية (د) ٥، وسيلة للموقع لتقديم إشعار بمقتضى الفقرة ١ (ب) من المادة ٨ من هذا القانون، وأن يضمن حيثما تقدم الخدمات بمقتضى الفقرة الفرعية (د) ٦ إتاحة خدمة إلغاء ناجزة،  
(و) أن يستخدم في أداء خدماته نظام وإجراءات وموارد بشرية جديرة بالثقة.
- ٢- يتحمل مقدم خدمات التصديق النتائج القانونية المترتبة على تخلفه عن الوفاء باشتراطات الفقرة ١.

#### الفقرة ١:

- ١٤٢- تعبر الفقرة الفرعية (أ) عن القاعدة الأساسية التي مفادها أن مقدم خدمات التصديق ينبغي أن يتقيد بما يقدمه، مثلاً، في بيان ممارسات التصديق لوفي أي نوع آخر من بيانات السياسات، من تأكيدات والتزامات
- ١٤٣- وتحدد الفقرة الفرعية (ج) المحتويات الجوهرية لأية شهادة تصدر بموجب القانون النموذجي، والمفعول الأساسي لتلك الشهادة. ويجدر

بالملاحظة أنه، في حالة التوقيعات الرقمية، يجب أن يكون بالوسع أيضا التحقق من ارتباط الموقع بالمفتاح العمومي، وكذلك بالمفتاح الخاص (انظر الوثيقة A/ CN. 9/484، الفقرة ٧١)، وتسرّد الفقرة الفرعية (د) عناصر إضافية يتعين أن تدرج في الشهادة أو أن يتاح للطرف المعول الحصول عليها أو الوصول إليها بطريقة أخرى، حيثما تكون ذات صلة بشهادة معينة. والفقرة الفرعية (هـ) ليس مقصودا منها أن تطبق على شهادات مثل شهادات "المعاملات"، أي الشهادات التي تخص معاملة واحدة، أو على الشهادات الزهيدة القيمة الخاصة باستخدامات قليلة المخاطرة، وكلا النوعين قد يكون خاضعا للإلغاء.

١٤٤- قد يعتقد أن الواجبات والالتزامات المنصوص عليها في المادة ٩ ربما يكون من المعقول أن يتوقع أن يتمثل لها أي مقدم خدمات تصديق، وليس من يصدون شهادات "عالية القيمة" فقط، بيد أن القانون النموذجي لا يشترط على الموقع أو مقدم خدمات التصديق درجة من العناية أو الجدارة بالثقة ليست لها علاقة معقولة بالأغراض التي يستخدم فيها التوقيع الإلكتروني أو الشهادة (انظر الفقرة ١٣٧ أعلاه) ولذلك يفضل القانون النموذج حلا يربط الالتزامات المبينة في المادتين ٨ و ٩ كلتيهما بإنتاج توقيعات إلكترونية ذات دلالة قانونية (انظر الوثيقة A/ CN. 9/483، الفقرة ١١٧). ويحصر نطاق المادة ٩ في المجموعة الواسعة من الأحوال التي تقدم فيها خدمات التصديق لتأييد توقيع إلكتروني يمكن أن يستخدم لإحداث مفعول قانوني كتوقيع، لا يرسي القانون النموذجي إلى إنشاء أنواع جديدة من المفاعيل القانونية للتوقيعات (انظر الوثيقة A/ CN. 9/483، الفقرة ١١٩).

#### الفقرة ٢:

١٤٥- بالتوازي مع الفقرة ١ من المادة ٨، تترك الفقرة ٢ للقانون الوطني الواجب التطبيق تحديد العواقب القانونية المترتبة على عدم الامتثال

للاستراطيات المبينة في الفقرة ١ (انظر الفقرة ١٤١ أعلاه والوثيقة A/ 56/ 17، الفقرة ٢٣٠). ورهنا بقواعد القانون الوطني المطبقة فإن مؤلفي الفقرة ٢ لا يقصدون أن تفسر تلك الفقرة باعتبارها قاعدة مسئولية مطلقة. ولا يتوخي أن يكون مفعول الفقرة ٢ هو استبعاد إمكانية قيام مقدم خدمات التصديق بالبرهان، مثلاً، علي عدم وجود تقصير أو مشاركة في تقصير.

١٤٦- وقد كانت مشاريع المادة ٩ تحتوي سابقاً علي فقرة إضافية تتناول نتائج المسئولية علي النحو المبين في الفقرة ٢. ولدى إعداد القانون النموذجي، لوحظ أن مسئولية مقدمي خدمات التصديق لن يتم تناولها بطريق كافية باعتماد حكم وحيد علي غرار الفقرة ٢. ففي حين أن الفقرة ٢ قد تنص علي مبدأ مناسب للتطبيق علي الموقعين، فإنها قد لا تكون كافية لتناول الأنشطة المهنية والتجارية التي تتناولها المادة ٩. وكان يمكن أن تتمثل إحدى سبل التعويض عن هذا النقص بأن تورد في نص القانون النموذجي قائمة بالعوامل التي ينبغي أن توضع في الاعتبار في تقدير أي خسارة ناتجة عن تخلف مقدم خدمات التصديق عن الوفاء باشتراطات الفقرة ١. وقد تقرر في النهاية أن تدرج في هذا الدليل قائمة غير حصرية بعوامل استرشادية. فلدي تقدير مسئولية مقدم خدمات التصديق، ينبغي أن توضع في الاعتبار العوامل التالية، علي سبيل المثال لا الحصر:

(أ) تكلفة الحصول علي الشهادة،

(ب) طبيعة المعلومات التي يجري التصديق عليها،

(ج) وجود ومدى أي قيد علي الغرض الذي يمكن أن تستخدم الشهادة من أجله،

(د) وجود أي بيان يجد من نطاق أو مدى مسئولية مقدم خدمات التصديق،

(هـ) أي سلوك إسهامي من جانب الطرف المعول. ولدى إعداد القانون

النموذجي، اتفق عموماً علي أنه، عندما تحدد في الدولة المشتري الخسارة

التي يمكن استردادها، ينبغي إيلاء الاعتبار للقواعد النازمة لحدود المسؤولية في الدولة التي يوجد فيها مقدم خدمات التصديق أو في أي دولة أخرى يطبق قانونها بموجب قاعدة تنازع القوانين ذات الصلة (انظر الوثيقة A/ CN. 9/484، الفقرة ٧٤).

#### الإحالات علي وثائق الأونيسترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢٢٣-٢٣٠، و ٢٦٤-٢٦٥ و ٢٨٤  
A/CN.9/493، المرفق، الفقرات ١٤٢-١٤٦،  
A/CN.9/484، الفقرات ٧٠-٧٤،  
A/CN.9/WG.IV/WP.88، المرفق، الفقرات ١٧٣-١٤١،  
A/ CN. 9/483، الفقرات ١١٤-١٢٧،  
A/CN.9/467، الفقرات ١٠٥-١٢٩،  
A/CN.9/WG.IV/WP.84، الفقرتان ٥٤-٦٠،  
A/CN.9/465، الفقرات ١٢٣-١٤٢ (مشروع المادة ١٢)،  
A/CN.9/WG.IV/WP.82، الفقرات ٥٩-٦٨ (مشروع المادة ١٢)،  
A/CN.9/457، الفقرات ١٠٨-١١٩،  
A/CN.9/WG.IV/WP.80، الفقرات ٢٢-٢٤،

#### المادة ١٠- الجدارة بالثقة

لأغراض الفقرة ١ (و) المادة ٩ من هذا القانون، يجوز، لدى تقرير ما إذا كانت أية نظم وإجراءات وموارد بشرية يستخدمها مقدم خدمات التصديق جديرة بالثقة، أو مدى جدارتها بالثقة، إيلاء الاعتبار للعوامل التالية:  
(أ) الموارد المالية والبشرية، بما في ذلك توافر الموجودات، أو

- (ب) جودة نظم المعدات والبرمجيات، أو
- (ج) إجراءات تجهيز الشهادات وطلبات الحصول علي الشهادة والاحتفاظ بالسجلات، أو
- (د) إتاحة المعلومات للموقعين المحددين في الشهادات وللأطراف المعولة المحتملة، أو
- (هـ) انتظام ومدى مراجعة الحسابات من جانب هيئة مستقلة، أو
- (و) وجود إعلان من الدولة أو من هيئة اعتماد أو من مقدم خدمات التصديق بخصوص الامتثال لما سبق ذكره أو بخصوص وجوده، أو
- (ز) أي عامل آخر ذي صلة.
- مرونة مفهوم الجدارة بالثقة:

١٤٧- كانت المادة ١٠ مصوغة في البداية كجزء من المادة ٩. وعلي الرغم من أن ذلك الجزء أصبح لاحقاً مادة منفصلة فإن المقصود منه أساساً هو أن يساعد علي تفسير المفهوم الذي تشير إليه عبارة "نظماً وإجراءات وموارد بشرية جديرة بالثقة" الوارد في الفقرة ١ (و) من المادة. والمادة ١٠ مصوغة كقائمة غير حصرية بعوامل ينبغي أن توضع في الاعتبار لدى البت في الجدارة بالثقة. والمقصود بالقائمة أن تقدم مفهوماً مرناً للجدارة بالثقة، يمكن أن يتغير محتواه تبعاً لما هو متوقع من الشهادة في السياق الذي تنشأ فيه.

#### الإحالات علي وثائق الأونسترال:

- الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢٣١-٢٣٤، و ٢٦٦-٢٧١ و ٢٨٤
- A/CN.9/493، المرفق، الفقرة ١٤٧،
- A/CN.9/WG.IV/WP.88، المرفق، الفقرة ١٤٢،



#### المادة ١١- سلوك الطرف المعول

يتحمل الطرف المعول النتائج القانونية الناجمة عن تخلفه عن:

(أ) اتخاذ خطوات معقولة للتحقق من قابلية التعويل على التوقيع الإلكتروني، أو

(ب) اتخاذ خطوات معقولة، إذا كان التوقيع الإلكتروني مؤيدا بشهادة،  
لأجل:

١- التحقق من صلاحية الشهادة أو وقفها أو إلغائها،

٢- مراعاة وجود أي قيد بخصوص الشهادة.

#### معقولة التعويل:

١٤٨- تجسد المادة ١١ فكرة أن الطرف الذي يعتزم أن يعول على توقيع إلكتروني ينبغي أن يضع في اعتباره مسألة ما إن كان ذلك التعويل معقولا، وإلى أي مدى هو كذلك في ضوء الظروف. وليس مقصودا منها أن تتناول مسألة صحة التوقيع الإلكتروني، التي يجري تناولها في إطار المادة ٦، والتي لا ينبغي أن تتوقف على سلوك الطرف المعول. فينبغي إبقاء مسألة صحة التوقيع الإلكتروني منفصلة عن مسألة ما إن كان من المعقول من الطرف المعول أن يعول على توقيع لا يستوفي المعيار المبين في المادة ٦.

#### مسائل المستهلكين:

١٤٩- في حين أن المادة ١١ يمكن أن تلقي عبئا على عاتق الأطراف المعولة وخصوصا عندما يكون أولئك الأطراف مستهلكين، فإنه يمكن أن يستذكر أن القانون النموذجي ليس مقصودا منه أن يعلو على أية قاعدة تحكم

حماية المستهلكين. غير أن القانون النموذجي يمكن أن يؤدي دوراً مفيداً في توعية جميع الأطراف المعنية، بما فيها الطرف المعولة، بشأن معيار السلوك المعقول الذي ينبغي استيفاؤه فيما يتعلق بالتوقعات الإلكترونية، وفضلاً عن ذلك فإن وضع معيار سلوك يتعين بموجبه علي الطرف المعول أن يتحقق من قابلية التعويل علي التوقيع بوسائل يسهل الوصول إليها يمكن أن يعتبر أمراً ضرورياً لإنشاء أي نظام مرفق مفاتيح عمومية.

#### مفهوم الطرف المعول:

١٥٠- يقصد من مفهوم "الطرف المعول"، وفقاً لتعريفه، أن يشمل أي طرف قد يعول علي توقيع إلكتروني، وعليه يمكن، رهناً بالظروف، أن يكون "الطرف المعول" أي شخص له علاقة تعاقدية بالموقع أو مقدم خدمات التصديق أو ليست له علاقة تعاقدية بهما، بل يمكن تصور أن يصبح مقدم خدمات التصديق نفسه أو الموقع نفسه طرفاً معولاً" غير أن المفهوم الواسع لعبارة "الطرف المعول" لا ينبغي أن يؤدي علي إلقاء التزام علي عاتق صاحب الشهادة بأن يتحقق من صحة الشهادة التي يشترها من مقدم خدمات التصديق.

#### التخلف عن الامتثال لاشتراطات المادة ١١:

١٥١- فيما يتعلق بالأثر الذي يمكن أن يترتب علي إرساء التزام عام علي عاتق الطرف المعول بأن يتحقق من صحة التوقيع الإلكتروني أو الشهادة، تنشأ مسألة الحالات التي يتخلف فيها الطرف المعول من الامتثال لاشتراطات المادة ١١. فإذا تخلف الطرف المعول عن الامتثال لتلك الاشتراطات، لا ينبغي منه ذلك الطرف من استخدام التوقيع أو الشهادة إذا لم يكن من شأن التحقق المعقول أن يكشف عدم صحة التوقيع أو الشهادة. ولا يقصد من اشتراطات المادة ١١ أن تشترط مراعاة القيود، أو التحقق من

المعلومات، التي لا يسهل على الطرف المعول الوصول إليها، وقد يلزم أن يعالج مثل هذه الحالة القانونية المطبق خارج نطاق القانون النموذجي. وبصفة أعم فإن نتائج عدم امتثال الطرف المعول لاشتراطات المادة ١١ تخضع للقانون المطبق خارج نطاق القانون النموذجي (انظر الوثيقة A/ CN. 9/484، الفقرة ٧٥) وفي ذلك الصدد، اعتمدت صيغة موازية في المادة ١١ وفي الفقرة ٢ من المادتين ٨ و ٩. وأثناء إعداد القانون النموذجي، اقترح التمييز بين النظام القانوني المطبق على الموقع ومقدم خدمات التصديق، من جهة (الذين ينبغي لكليهما أن يواجهوا الالتزامات المتعلقة بسلوكها في سياق عملية التوقيع الإلكتروني)، والنظام المطبق على الطرف المعول، من جهة أخرى (الذي قد يكون من المناسب أن يرسى القانون النموذجي بشأنه قواعد سلوك ولكن لا ينبغي تعريضه للمستوى ذاته من الالتزامات مثل الطرفين الآخرين). غير أن الرأي السائد تمثل في أن مسألة إقامة هذا التمييز ينبغي أن تترك للقانون المطبق خارج إطار القانون النموذجي<sup>(١)</sup>.

#### الإحالات على وثائق الأونيسترال:

الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢٣٥-٢٣٦، و ٢٦٨-٢٦٩ و ٢٨٤  
A/CN.9/493، المرفق، الفقرات ١٤٨-١٥١،  
A/CN.9/484، الفقرة ٧٥،  
A/CN.9/WG.IV/WP.88، المرفق، الفقرات ١٤٣-١٤٦،  
A/CN.9/467، الفقرات ١٣٠-١٤٣،  
A/CN.9/WG.IV/WP.84، الفقرات ٦١-٦٣،

(١) المرجع نفسه، الفقرتان ٢٢٠ و ٢٢١.

A/CN.9/465، الفقرات ١٠٩-١٢٢ (مشروعا المادتين ١٠ و ١١)،  
A/CN.9/WG.IV/WP.82، الفقرات ٥٦-٥٨ (مشروعا المادتين ١٠  
و ١١)،

A/CN.9/457، الفقرات ٩٩-١٠٧،

A/CN.9/WG.IV/WP.80، الفقرتان ٢٠ و ٢١.

#### المادة ١٢- الاعتراف بالشهادات والتوقيعات الإلكترونية الأجنبية

١- لدى تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني ساري المفعول قانونياً، أو مدى كونهما كذلك، لا يولي أي اعتبار لما يلي:  
(أ) الموقع الجغرافي. الذي تصدر فيه الشهادة أو ينشأ أو يستخدم فيه التوقيع الإلكتروني، أو

(ب) الموقع الجغرافي لمكان عمل المصدر أو الموقع.

٢- يكون للشهادة التي تصدر خارج (الدولة المشترعة) نفس المفعول القانوني في (الدولة المشترعة) الذي للشهادة التي تصدر في (الدولة المشترعة) إذا كانت تتبع مستوى مكافئاً جوهرياً من قابلية التعويل.

٣- يكون للتوقيع الإلكتروني الذي ينشأ أو يستخدم خارج (الدولة المشترعة) نفس المفعول القانوني (في الدولة المشترعة) الذي للتوقيع الإلكتروني الذي ينشأ أو يستخدم في (الدولة المشترعة) إذا كان يتبع مستوى مكافئاً جوهرياً من قابلية التعويل.

٤- لدى تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني يتحان مستوى مكافئاً جوهرياً من قابلية التعويل لأغراض الفقرتان ٢ أو ٣، يولي الاعتبار للمعايير الدولية المعترف بها ولأية عوامل أخرى ذات صلة.

٥- إذا اتفقت الأطراف فيما بينها، برغم ما ورد في الفقرات ٢ و ٣ و ٤، علي استخدام أنواع معينة من التوقيعات الإلكترونية أو الشهادات، يتعين

الاعتراف بذلك الاتفاق باعتباره كافياً لأغراض الاعتراف عبر الحدود، ما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضى القانون المطبق.

#### القاعدة العامة لعدم التمييز:

١٥٢- المقصود بالفقرة ١ أن تجسد المبدأ الأساسي الذي مفاده أن مكان المنشأ، في حد ذاته، لا ينبغي أن يكون، بأي طريقة، عاملاً يحدد ما عن كان، وإلى أي مدى، ينبغي الاعتراف بالشهادات أو التوقيعات الإلكترونية الأجنبية باعتبارها قابلة لأن تكون سارية المفعول قانونياً، وإلى أي مدى ينبغي ذلك. ولا ينبغي أن يتوقف تحديد ما عن كانت الشهادة قابلة لأن تكون سارية المفعول قانونياً أو التوقيع الإلكتروني قابلاً لأن يكون ساري المفعول قانونياً، وإلى أي مدى ينبغي ذلك، على المكان الذي صدرت فيه الشهادة أو التوقيع الإلكتروني (انظر الوثيقة A/ CN. 9/484، الفقرة ٢٧) بل على قابلية التعويل التقنية عليها.

#### مستوى مكافئاً جوهرياً من قابلية التعويل:

١٥٣- الغرض من الفقرة ٢ هو توفير معيار عام للاعتراف بالشهادات عبر الحدود، الذي إذا لم يوجد ربما واجه مقدم خدمات التصديق عبثاً غير معقول يتمثل في الاضطرار على الحصول على تراخيص في ولايات قضائية متعددة، ولكن لا يقصد بالفقرة ٢ أن تضع مقدمي خدمات التصديق الأجانب في موضوع أفضل من نظرائهم المحليين<sup>(١)</sup>. ولهذا الغرض، تضع الفقرة ٢ حد أدنى للتكافؤ التقني للشهادات الأجنبية يستند على اختيار قابلية التعويل عليها على أساس شروط الموثوقية التي تضعها الدولة المشترعة عملاً بالقانون النموذجي (انظر الوثيقة A/ CN. 9/483، الفقرة ٣١).

(١) لمرجع نفسه، الفقرة ٢٨٢.

وينبغي أن يطبق ذلك المعيار دون اعتبار لطبيعة مخطط التصديق المطبق في الولاية القضائية التي صدرت منها الشهادة أو التوقيع (انظر الوثيقة A/ CN. 9/483، الفقرة ٢٩).

تفاوت مستوى قابلية التعويل حسب الولاية القضائية:

١٥٤- من خلال الإشارة على المفهوم الأساسي الذي تدل عليه عبارة "مستوى مكافئاً جوهرياً من قابلية التعويل"، تسلم الفقرة ٢ بإمكانية وجود تفاوت كبير في الشروط المطلوب بين كل من الولايات القضائية على حدة. ولا يعني اشتراط التكافؤ، كما هو مستخدم في الفقرة ٢، أن مستوى قابلية التعويل على الشهادة الأجنبية ينبغي أن يكون مطابقاً تماماً لمستوى قابلية التعويل على الشهادة المحلية (المصدر نفسه، الفقرة ٣٢).

تفاوت مستوى قابلية التعويل داخل الولاية القضائية:

١٥٥- ينبغي أن يلاحظ، علاوة على ذلك، أن مقدمي خدمات التصديق يصدرهم، في الممارسة العلمية، شهادات ذات مستويات متفاوتة من قابلية التعويل عليها، وفقاً للغرض الذي يقصد أن يستخدم الزبائن الشهادات فيه. وتبعاً لمستوى قابلية التعويل على كل شهادة على حدة، يمكن أن تحدث الشهادات والتوقيعات الإلكترونية مفاعيل قانونية متفاوتة، سواء داخلية أم في الخارج، فمثلاً، في بلدان معينة، يمكن حتى للشهادات التي تسمى أحياناً "منخفضة المستوى" أو "منخفضة القيمة" أن تحدث مفاعيل قانونية في ظروف معينة (مثلاً عندما يكون الطرفان قد اتفقا تعاقدية على استخدام تلك الصكوك) (انظر الوثيقة A/ CN. 9/484، الفقرة ٧٧). ولذلك ينبغي أن يوضع في الاعتبار، لدى تطبيق مفهوم التكافؤ كما هو مستخدم في الفقرة ٢، أن التكافؤ الذي يلزم إثباته هو التكافؤ بين الشهادات المتشابهة وظيفياً. وغير أنه لم تبذل محاولة في القانون النموذجي لإرساء تناظر بين الشهادات المختلفة الأنواع

التي يصدرها مقدمو خدمات تصديق مختلفون في ولايات قضائية شتى. وقد صيغ القانون النموذجي بحيث يتوخى إمكانية التفاوت في الرتب بين مختلف أنواع الشهادات. وفي الممارسة العملية، تعتمد عادة المحكمة أو هيئة التحكيم التي يطلب منها أن تبت في المفعول القانوني لشهادة أجنبية على النظر في كل شهادة على حدة على أساس جدارتها وتحاول أن تعادل بينها وبين أقر بمستوى مناظر في الدولة المشترعة (انظر الوثيقة A/ CN. 9/483، الفقرة ٣٣).

**المعاملة المتساوية للشهادات وللأنواع الأخرى من التوقيعات الإلكترونية:**

١٥٦- تعبر الفقرة ٣ فيما يتعلق بالتوقيعات الإلكترونية عن نفس القاعدة المبينة في الفقرة ٢ بشأن الشهادات (A/ CN. 9/483، الفقرة ٤١).

**الاعتراف بمفعول قانوني ما للامتثال لقوانين بلد أجنبي:**

١٥٧- لا تتناول الفقرتان ٢ و ٣ سوى اختبار قابلية التعويل عبر الحدود الذي ينبغي أن يطبق لدى تقييم قابلية التعويل على شهادة أجنبية أو توقيع إلكتروني أجنبي. غير أنه، لدى إعداد القانون النموذجي، روعي أن الدول المشترعة قد ترغب في إلغاء الاحتياج على اختبار قابلية التعويل فيما يتعلق بتوقيعات أو شهادات كمعينة عندما تكون الدولة المشترعة مقتنعة بأن قانون الولاية القضائية التي تنشأ منها التوقيع أو الشهادة يوفر معيارا كافيا لقابلية التعويل. وبشأن الأساليب القانونية التي يمكن بها للدولة المشترعة أن تعترف مسبقا بقابلية التعويل على الشهادات والتوقيعات التي تتمثل لقانون بلد أجنبي (مثلا إعلان من طرف واحد أو معاهدة)، لا يحتوي القانون النموذجي على اقتراح محدد (انظر الوثيقة A/ CN. 9/483، الفقرتان ٣٩ و ٤٢).

العوامل التي ينبغي النظر فيها لدى تقييم التكافؤ الجوهرى للشهادات والتوقيعات الأجنبية:

١٥٨- لدى إعداد القانون النموذجي، صيغت الفقرة ٤ في البداية في شكل قائمة بالعوامل التي ينبغي وضعها في الاعتبار عند البت في ما إن كانت الشهادة أو التوقيع الإلكتروني يتحان مستوى من قابلية التعويل مكافئا جوهريا فيما يتعلق بأغراض الفقرة ٢ أو الفقرة ٣. ووجد لاحقا أن معظم هذه العوامل مدرج بالفعل في المواد ٦ و ٩ و ١٠. ورثي أن النص مجددا علي تلك العوامل في سياق المادة ١٢ سيكون لا داعي له. ووجد أن الإحالة، بدلا من ذلك، في الفقرة ٤، علي أحكام القانون النموذجي ذات الصلة، التي تذكر فيها المعايير المعنية، وربما مع إضافة معايير أخرى ذات أهمية خاصة للاعتراف عبر الحدود، ستؤدي إلي صياغة مفرطة التعقيد (انظر، علي الخصوص، الوثيقة A/ CN. 9/483، الفقرات ٤٣ - ٤٩). في نهاية المطاف، حولت الفقرة ٤ إلي إشارة غير محددة إلي "أية عوامل أخرى ذات صلة"، ومن بين تلك العوامل تنضم العوامل المذكورة في المواد ٦ و ٩ و ١٠ فيما يتعلق بتقديم الشهادات والتوقيعات الإلكترونية الداخلية بأهمية خاصة. وعلاوة علي ذلك، تراعي الفقرة ٤ النتائج المترتبة علي كون تقييم تكافؤ الشهادات الأجنبية يختلف بعض الاختلاف عن تقييم جدارة التصديق بالنقطة بموجب المادتين ٩ و ١٠. ولذلك أضيفت في الفقرة ٤ إشارة إلي "المعايير الدولية المعترف بها".

#### المعايير الدولية المعترف بها:

١٥٩- ينبغي تفسير عبارة "معياري دولي معترف به" تفسيراً واسعاً لتشمل المعايير الدولية للتقنية والتجارية (أي المعايير المنبثقة عن السوق) وكذلك المعايير والقواعد التي اعتمدها هيئات حكومية أو دولية حكومية (A/ CN. 9/483، الفقرة ٤٩) و "المعايير الطوعية" (كما هي موصوفة في الفقرة ٦٩



أعلامه<sup>(١)</sup> ويمكن أن يكون "المعيار الدولي المعترف به" بيانات الممارسات التقنية أو القانونية أو التجارية المقبولة، التي وضعها القطاع العام أو القطاع الخاص (أو كلاهما)، ذات الطبيعة المعيارية أو التفسيرية، المقبولة عموماً باعتبارها منطبقة على الصعيد الدولي. ويمكن أن تكون تلك المعايير في شكل اشتراطات أو توصيات أو مبادئ توجيهية أو مدونات قواعد سلوك أو بيانات لأفضل الممارسات أو أفضل المعايير (A/ CN. 9/483، الفقرة ١٠١-١٠٤).

الاعتراف بالاتفاقات المبرمة بين الأطراف المعنية:

١٦٠- تنص الفقرة ٥٤ على الاعتراف بالاتفاقات المبرمة بين الأطراف المعنية بشأن استخدام أنواع معينة من التوقيعات الإلكترونية أو الشهادات باعتبار تلك الاتفاقات أساساً كافياً للاعتراف عبر الحدود (فيما بين تلك الأطراف بتلك التوقيعات أو الشهادات المتفق عليها (A/ CN. 9/483، الفقرة ٥٤)). وينبغي أن يلاحظ أنه، اتساقاً مع المادة ٥، لا يقصد من الفقرة ٥ أن تحل محل أي قانون إلزامي، وخصوصاً أي اشتراط إلزامي للتوقيعات الخطية قد ترغب الدول المشتركة في أن تحافظ عليه في القانون المطبق (A/ CN. 9/483، الفقرة ١١٣). والفقرة ٥ لازمة فضاء مفعول للشروط التعاقدية التي قد يتفق بموجبها الأطراف، فيما بينهم، على الاعتراف باستخدام توقيعات إلكترونية أو شهادات معينة (يمكن أن تعبر أجنبية في بعض أو جميع الدول التي قد يسعى الأطراف إلى الحصول فيها على اعتراف قانوني بتلك التوقيعات أو الشهادات)، دون إخضاع تلك التوقيعات أو الشهادات لاختبار التكافؤ الجوهرية المبين في الفقرات ٢ و ٣ و ٤. ولا تمس الفقرة ٥ الوضع القانوني للأطراف الثلاثة (A/ CN. 9/483، الفقرة ٥٦).

---

(١) المرجع نفسه، الفقرة ١٧٨.

الإحالات علي وثائق الأونيسترال:

- الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17) الفقرات ٢٣٧، و ٢٧٠-٢٧٣ و ٢٨٤،  
A/CN.9/493، المرفق، الفقرات ١٥٢-١٦٠،  
A/CN.9/484، الفقرات ٧٦-٧٨،  
A/CN.9/WG.IV/WP.88، المرفق، الفقرات ١٤٧-١٥٥،  
A/ CN. 9/483، الفقرات ٢٥-٥٨ (المادة ١٢)،  
A/ CN.9/ WG. IV/ WP 84 و ٨٤، الفقرتان ٤٩-٥١،  
A/ CN. 9/ 465، الفقرات ٦١-٦٨ (مشروع المادة ١٣)،  
A/ CN. 9/ 465، الفقرات ٢١-٣٥،  
A/ CN.9/ WG. IV/ WP, 82، الفقرات ٦٩-٧١،  
A/CN.9/454، الفقرة ١٧٣،  
A/CN.9/446، الفقرات ١٩٦-٢٠٧ (مشروع المادة ١٩)،  
A/CN.9/WG.IV/WP.73، الفقرة ٧٥،  
A/CN.9/WG.IV/WP.71، الفقرات ٧٣-٧٥،

### ٣- اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات

#### الإلكترونية في العقود الدولية

إن الجمعية العامة،

إذ تشير إلى قرارها ٢٢٠٥ (د-٢١) المؤرخ ١٧ كانون الأول/ ديسمبر ١٩٦٦ الذي أنشأت بموجبه لجنة الأمم المتحدة للقانون التجاري الدولي مسندة إليها ولاية زيادة التنسيق والتوحيد التدريجين للقانون التجاري الدولي، مع الأخذ في الاعتبار، في ذلك الصدد، مصالح جميع الشعوب، وبخاصة شعوب البلدان النامية في تنمية التجارة الدولية تنمية واسعة النطاق.

وإذ تری أن المشاكل الناجمة عن التشكك في القيمة القانونية لاستخدام الخطابات الإلكترونية في سياق العقود الدولية تشكل عقبة أمام التجارة الدولية،

واقتراعاً منها بأن اعتماد قواعد موحدة لإزالة العقبات القائمة أمام استخدام الخطابات الإلكترونية في العقود الدولية، بما فيها العقبات التي قد تنشأ عن أعمال صكوك القانون التجاري الدولي الحالية، من شأنه أن يعزز التيقن القانوني وإمكانية التسبؤ بمصائر العقود الدولية من الناحية التجارية وقد يساعد الدول على اكتساب القدرة على النفاذ إلى دروب التجارة الحديثة،

وإذا تشير إلى أن اللجنة قررت، في دورتها الرابعة والثلاثين المعقودة في عام ٢٠٠١ أن تعد صكاً دولياً يتناول مسائل التعاقد الإلكتروني، على أن يهدف أيضاً إلى إزالة العقبات أمام التجارة الإلكترونية في الاتفاقيات والاتفاقيات التجارية التي تشكل القوانين الموحدة الحالية، وعهدت إلى فريقها العامل الرابع المعني بالتجارة الإلكترونية بإعداد مشروع بذلك الشأن<sup>(١)</sup>.

(١) الوثائق الرسمية للجمعية العامة، الدورة السادسة والخمسون، الملحق رقم ١٧ (A/56/17 و Corr 3)، الفقرات ٢٩١-٢٩٥.

وإذ تلاحظ أن الفريق العامل كرس ست دورات عقدت في الأعوام ٢٠٠٢ إلى ٢٠٠٤، لإعداد مشروع اتفاقية بشأن استخدام الخطابات الإلكترونية في العقود الدولية، وأن اللجنة نظرت في مشروع الاتفاقية في دورتها الثامنة والثلاثين المعقودة في عام ٢٠٠٥<sup>(١)</sup> وإذ تدرك أن جميع الدول والمنظمات الدولية المهتمة قد دُعيت إلى المشاركة في إعداد مشروع الاتفاقية في جميع دورات الفريق العامل وفي دورة اللجنة الثامنة والثلاثين بصفة أعضاء أو مراقبين، وأُتيحت لها فرصة كاملة للتكلم وتقديم الاقتراحات،

وإذ تلاحظ مع الارتياح أنه جري تعميم نص مشروع الاتفاقية على جميع الحكومات والمنظمات الدولية التي دُعيت إلى حضور اجتماعات اللجنة والفريق العامل بصفة مراقبين لإبداء تعليقات عليه قبل انعقاد دورة اللجنة الثامنة والثلاثين، وأن التعليقات الواردة كانت معروضة على اللجنة في دورتها الثامنة والثلاثين<sup>(٢)</sup>.

وإذ تحيط علماً مع الارتياح بالقرار الذي اتخذته اللجنة في دورتها الثامنة والثلاثين بتقديم مشروع الاتفاقية إلى الجمعية العامة للنظر فيه<sup>(٣)</sup>.

وإذ تحيط علماً بمشروع الاتفاقية الذي وافقت عليه اللجنة.

١- تعرف عن تقديرها للجنة الأمم المتحدة للقانون التجاري الدولي لإعدادها مشروع الاتفاقية بشأن استخدام الخطابات الإلكترونية في العقود الدولية<sup>(٤)</sup>.

(١) المرجع نفسه، الدورة الستون، الملحق رقم ١٧ (A/60/17) الفصل الثالث.

(٢) A. CN. 9/ 578 و add. 1- 17.

(٣) الوثائق الرسمية للجمعية العامة، الدورة الستون، الملحق رقم ١٧ (A/60 / 17)، الفقرة ١٦٧.

(٤) المرجع نفسه، المرفق الأول.

٢- تعتمد اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية، الواردة في مرفق هذا القرار، وتطلب إلى الأمين العام أن يفتح باب التوقيع عليها؛

٣- تهيب بجميع الحكومات النظر في أن تصبح أطرافاً في الاتفاقية.

الجلسة العامة ٥٣

٢٣ تشرين الثاني/نوفمبر ٢٠٠٥

## المرفق

### اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات

#### الإلكترونية في العقود الدولية

إن الدول الأطراف في هذه الاتفاقية،

إذ تؤكد من جديد اقتناعها بأن التجارة الدولية القائمة على المساواة والمنفعة المتبادلة تمثل عنصراً مهماً في تعزيز العلاقات الدولية بين الدول،  
وإذ تلاحظ أن ازدياد استخدام الخطابات الإلكترونية يحسن كفاءة الأنشطة التجارية ويعزز الأواصر التجارية وبتح فرص وصول جديدة إلى أطراف وأسواق كانت نائية في الماضي، ويؤدي بالتالي دوراً جوهرياً في تعزيز التجارة والتنمية الاقتصادية داخلياً ودولياً على حد سواء،  
وإذ تضع في اعتبارها أن المشاكل الناشئة عن التشكك في القيمة القانونية لاستخدام الخطابات الإلكترونية في العقود الدولية تمثل عائقاً أمام التجارة الدولية،

واقتراعاً منها بأن اعتماد قواعد موحدة لإزالة العقبات القائمة أمام استخدام الخطابات الإلكترونية في العقود الدولية، بما فيها العقبات التي قد تنشأ عن أعمال صكوك القانون التجاري الدولي الحالية، من شأنه أن يعزز التيقن القانوني وقابلية التنبؤ بمصائر العقود الدولية من الناحية التجارية وأن يساعد الدول على اكتساب القدرة على النفاذ إلى دروب التجارة الحديثة،

وإذ تري أن القواعد الموحدة ينبغي أن تحترم حرية الأطراف في اختيار الوسائط والتكنولوجيات الملائمة، مع مراعاة مبدأي الحياد التكنولوجي والشفاف الوظيفي، ما دامت الوسائل التي تختارها الأطراف تقي بأغراض القواعد القانونية ذات الصلة،

ورغبة منها في توفير حل عام لتجاوز العقوبات القانونية أمام استخدام  
الخطابات الإلكترونية علي نحو مقبول للدول ذات النظم القانونية والاجتماعية  
والاقتصادية المختلفة،  
قد اتفقت علي ما يلي:





## **الفصل الأول**

### **مجال الانطباق**

#### **المادة ١**

##### **نطاق الانطباق**

- ١- تنطبق هذه الاتفاقية علي استخدام الخطابات الإلكترونية في سياق تكوين أو تنفيذ عقد بين أطراف تقع مقر عملها في دول مختلفة.
- ٢- يصرف النظر عن وقوع مقر عمل الأطراف في دول مختلفة عندما لا تتبين هذه الحقيقة من العقد أو من أي تعاملات بين الأطراف أو من المعلومات التي تنصح عنها الأطراف في أي وقت قبل إبرام العقد أو عند إبرامه.
- ٣- لا تؤخذ جنسية الأطراف ولا الصفة المدنية أو التجارية للأطراف أو للعقد في الاعتبار لدى تقرير انطباق هذه الاتفاقية.

#### **المادة ٢**

##### **الاستبعادات**

- ١- لا تنطبق هذه الاتفاقية علي الخطابات الإلكترونية المتعلقة بأي مما يلي:
  - (أ) العقود المبرمة لأغراض شخصية أو عائلية أو منزلية؛
  - (ب) "١" المعاملات المتعلقة بتبادل خاضع للوائح تنظيمية؛
  - "٢" معاملات النقد الأجنبي؛

٣- نظم الدفع فيما بين المصارف أو اتفاقات الدفع فيما بين المصارف، أو نظم المقاصة والتسوية المتعلقة بالأوراق المالية أو غيرها من الأصول أو الصكوك المالية؛

٤- إحالة الحقوق الضمانية في بيع الأوراق المالية أو غيرها من الأصول أو الصكوك المالية المودعة لدى وسيط أو إقراضها أو إيداعها أو الاتفاق على إعادة شرائها.

٢- لا تنطبق هذه الاتفاقية على السفائح (الكبيالات) أو السندات الإلكترونية أو بيانات الشحن أو سندات الشحن أو إيصالات المستودعات أو أي مستند قابل للإحالة أو صك يعطي حاملة أو المستفيد منه حقاً في المطالبة بتسليم بضاعة أو بدفع مبلغ من المال.

## **المادة ٢**

### **حرية الأطراف**

يجوز للأطراف استبعاد سريان هذه الاتفاقية أو الخروج عن أي من أحكامها أو تغيير مفعوله.

## **الفصل الثاني**

### **أحكام عامة**

## **المادة ٤**

### **التعريف**

لأغراض هذه الاتفاقية:

(أ) يقصد بتعبير "الخطاب" أي بيان أو إعلان أو مطلب أو إشعار أو طلب، بما في ذلك أي عرض وقبول عرض، يتعين على الأطراف توجيهه أو تختار توجيهه في سياق تكوين العقد أو تنفيذه؛

(ب) يقصد بتعبير "الخطاب الإلكتروني" أي خطاب توجهه الأطراف بواسطة رسائل بيانات؛

(ج) يقصد بتعبير "رسالة البيانات" المعلومات المنشأة أو المرسلة أو المستقاة أو المخزنة بوسائل إلكترونية أو مغناطيسية أو بصرية أو بوسائل مشابهة تشمل، على سبيل المثال لا الحصر، التبادل الإلكتروني أو البرق أو التلكس أو النسخ البرقي؛

(د) يقصد بتعبير "منشئ" الخطاب الإلكتروني الطرف الذي أرسل الخطاب الإلكتروني أو أنشأه قبل تخزينه، إن حدث تخزين، أو من قام بذلك نيابة عنه، ولكنه لا يشمل الطرف الذي يتصرف كوسيط فيما يخص ذلك الخطاب الإلكتروني؛

(هـ) يقصد بـ "المرسل إليه" فيما يتعلق بخطاب إلكتروني، الطرف الذي يريده المنشئ أن يتلقى الخطاب الإلكتروني، ولكنه لا يشمل الطرف الذي يتصرف كوسيط فيما يخص ذلك الخطاب الإلكتروني؛

(و) يقصد بتعبير "نظام معلومات" نظام لإنشاء رسائل البيانات أو إرسالها أو تلقيها أو تخزينها أو معالجتها على أي نحو آخر؛

(ز) يقصد بتعبير "نظام رسائل آلي" برنامج حاسوبي أو وسيلة إلكترونية أو وسيلة آلية أخرى تستخدم لاستهلاك إجراء ما أو للاستجابة كلياً أو جزئياً لرسائل بيانات أو لعمليات تنفيذها، دون مراجعة أو تدخل من شخص طبيعي في كل مرة يستهل فيها النظام إجراء ما أو ينشئ استجابة ما؛

(ح) يقصد بتعبير "مقر العمل" أي مكان يحتفظ فيه الطرف بمنشأة غير عارضة لمزاولة نشاط اقتصادي غير التوفير المؤقت لسلع أو خدمات من مكان معين.

## المادة ٥

### التفسير

- ١- لدى تفسير هذه الاتفاقية، يولي اعتبار لطابعها الدولي ولضرورة تعزيز الاتساق في تطبيقها ومراعاة حسن النية في التجارة الدولية.
- ٢- المسائل المتعلقة بالأمور التي تحكمها هذه الاتفاقية ولكن لا تحسمها بوضوح تسوي وفقا للمبادئ العامة التي تقوم عليها، أو وفقا للقانون المنطبق بمقتضى قواعد القانون الدولي الخاص، في حال عدم وجود مثل تلك المبادئ.

## المادة ٦

### مكان الأطراف

- ١- لأغراض هذه الاتفاقية، يفترض أن يكون مقر عمل الطرف هو المكان الذي يعينه ذلك الطرف، ما لم يثبت طرف آخر أن الطرف الذي عين ذلك المكان ليس له مقر عمل فيه.
- ٢- إذا لم يعين الطرف مقر عمل وكان له أكثر من مقر عمل واحد، كان مقر العمل، لأغراض هذه الاتفاقية، هو المقر الأوثق صلة بالعقد المعني، مع إيلاء اعتبار للظروف التي كانت الأطراف علي علم بها أو تتوقعها في أي وقت قبل إبرام العقد أو عند إبرامه.
- ٣- إذا لم يكن للشخص الطبيعي مقر عمل، أخذ بمحل إقامته المعتاد.
- ٤- لا يكون المكان مقر عمل لمجرد أنه: (أ) توجد فيه المعدات والتكنولوجيا الداعمة لنظام المعلومات الذي يستخدمه الطرف في سياق تكوين العقد؛ أو (ب) يمكن فيه لأطراف أخرى أن تصل إلي نظام المعلومات المعني.

٥- إن مجرد استخدام الطرف اسم نطاق أو عنوان بريد إلكتروني ذا صلة ببلد معين لا ينشئ قرينة علي أن مقر عمله يوجد في ذلك البلد.

## **المادة ٧**

### **اشتراطات الإبلاغ**

ليس في هذه الاتفاقية ما يمس بانطباق أي قاعدة قانونية قد تلزم الأطراف بالإفصاح عن هويتها أو مقار عملها أو عن معلومات أخرى، أو ما يعفي أي طرف من العواقب القانونية لتقديم بيانات غير دقيقة أو ناقصة أو كاذبة في ذلك الصدد.

## **الفصل الثالث**

### **استخدام الخطابات الإلكترونية في العقود الدولية**

## **المادة ٨**

### **الاعتراف القانوني بالخطابات الإلكترونية**

١- لا يجوز إنكار صحة الخطاب أو العقد أو إمكانية إنفاذه لمجرد كونه في شكل خطاب إلكتروني.

٢- ليس في هذه الاتفاقية ما يلزم أي طرف باستخدام الخطابات الإلكترونية أو قبولها، ولكن يجوز الاستدلال علي موافقة الطرف علي ذلك من سلوك ذلك الطرف.

## **المادة ٩**

### **اشتراطات الشكل**

١- ليس في هذه الاتفاقية ما يشترط إنشاء الخطاب أو تكوين العقد أو إثباتهما في أي شكل معين.

٢- حيثما يشترط القانون أن يكون الخطاب أو العقد كتابيا، أو ينص علي عواقب لعدم وجود كتابة، يعتبر ذلك الاشتراط قد استوفي بالخطاب الإلكتروني إذا كان الوصول إلي المعلومات الواردة فيه متيسرا علي نحو يتيح استخدامها في الرجوع إليها لاحقا.

٣- حيثما يشترط القانون أن يكون الخطاب أو العقد ممهورا بتوقيع طرف ما، أو ينص علي عواقب لعدم وجود توقيع، يستوفي ذلك الاشتراط فيما يخص الخطاب الإلكتروني إذا:

(أ) استخدمت طريقة ما لتعيين هوية الطرف المعني وتبين نية ذلك الطرف فيما يخص المعلومات الواردة في الخطاب الإلكتروني؛  
(ب) وكانت الطريقة المستخدمة:

١' موثوق بها بقدر مناسب للغرض الذي أنشئ الخطاب الإلكتروني أو أرسل من أجله، في ضوء كل الملابسات، بما فيها أي اتفاق ذي صلة؛ أو  
٢' قد أثبتت فعلياً بحد ذاتها أو مقترنة بأدلة إضافية، إنها أوفت بالوظائف المذكورة في الفقرة الفرعية (أ) أعلاه.

٤- حيثما يشترط القانون وجوب إتاحة الخطاب أو العقد أو الاحتفاظ به في شكله الأصلي، أو ينص علي عواقب لعدم وجود مستند أصلي، يعتبر ذلك الاشتراط قد استوفي فيما يخص الخطاب الإلكتروني إذا:

(أ) وجدت وسيلة موثوق بها تؤكد سلامة المعلومات الواردة فيه منذ الوقت الذي أنشئ فيه أولا في شكله النهائي، كخطاب إلكتروني أو غير ذلك؛  
(ب) وكانت المعلومات الواردة فيه، حيثما يشترط أن تكون متاحة، قابلة للعرض علي الشخص الذي يتعين أن تتاح له.

٥- لأغراض الفقرة ٤ (أ):

(أ) تكون معايير تقييم سلامة المعلومات هي ما إذا كانت تلك المعلومات قد ظلت كاملة ودون تحويل، بصرف النظر عن إضافة أي مصادقة وأي تغيير ينشأ في السياق المعتاد للإرسال والتخزين والعرض؛  
(ب) تقدر درجة الموثوقية المطلوبة في ضوء الغرض الذي أنشئت المعلومات من أجله وفي ضوء جميع الظروف ذات الصلة.

## المادة ١٠

### وقت ومكان إرسال الخطابات الإلكترونية وتلقيها

١- وقت إرسال الخطاب الإلكتروني هو الوقت الذي يغادر فيه ذلك الخطاب نظام معلومات يقع تحت سيطرة المنشئ أو الطرف الذي أرسل الخطاب نيابة عن المنشئ، أو وقت تلقي الخطاب الإلكتروني إذا لم يكن قد غادر نظام معلومات يقع تحت سيطرة المنشئ أو الطرف الذي أرسل الخطاب نيابة عن المنشئ.

٢- وقت تلقي الخطاب الإلكتروني هو الوقت الذي يصبح فيه ذلك الخطاب قابلاً للاستخراج من جانب المرسل إليه علي عنوان إلكتروني يعينه المرسل إليه. ووقت تلقي الخطاب الإلكتروني علي عنوان إلكتروني آخر للمرسل إليه هو الوقت الذي يصبح فيه الخطاب الإلكتروني قابلاً للاستخراج من جانب المرسل إليه علي ذلك العنوان ويصبح المرسل إليه علم بأن الخطاب الإلكتروني قد أرسل إلي ذلك العنوان. ويفترض أن يكون الخطاب الإلكتروني قابلاً للاستخراج من جانب المرسل إليه عندما يصل ذلك الخطاب إلي العنوان الإلكتروني للمرسل إليه.

٣- يعتبر الخطاب الإلكتروني قد أرسل من المكان الذي يوجد فيه مقر عمل المنشئ، ويعتبر قد تلقى في العنوان الذي يوجد فيه مقر عمل، المرسل إليه، حسبما تقررهما المادة ٦.

٤- تنطبق الفقرة ٢ من هذه المادة بصرف النظر عن احتمال أن يكون المكان الذي يوجد فيه نظام المعلومات الداعم لعنوان إلكتروني مغايراً للمكان الذي يعتبر الخطاب الإلكتروني قد تلقى فيه بمقتضى الفقرة ٣ من هذه المادة.

## **المادة ١١**

### **الدعوات إلى تقديم عروض**

أي اقتراح يقدم لإبرام عقد بواسطة خطاب إلكتروني واحد أو أكثر ولا يكون موجهاً إلى طرف معين واحد أو أكثر، بل يتيسر الاطلاع عليه للأطراف التي تستخدم نظم المعلومات، بما في ذلك الاقتراحات التي تستخدم تطبيقات تفاعلية لتقديم طلبات من خلال نظم معلومات من ذلك القبيل، يعتبر مجرد دعوى إلى تقديم عروض، ما لم يدل بوضوح على أن مقدم الاقتراح ينوي الالتزام به في حال قبوله.

## **المادة ١٢**

### **استخدام نظام الرسائل الآلية في تكوين العقود**

لا يجوز إنكار صحة أو إمكانية إنفاق العقد الذي يكون بالتفاعل بين نظام رسائل آلي وشخصي طبيعي، أو بالتفاعل بين نظامي رسائل آليين، لمجرد عدم مراجعة شخص طبيعي كلا من الأفعال التي قامت بها نظم الرسائل الآلية أو العقد الناتج عن تلك الأفعال أو تدخله فيها.

## **المادة ١٣**

### **إتاحة شروط العقد**

ليس في هذه الاتفاقية ما يمس بانطباق أي قاعدة قانونية قد تلزم الطرف الذي يتفاوض على بعض شروط العقد أو كلها من خلال تبادل خطابات إلكترونية بأن يتيح للطرف الآخر الخطابات الإلكترونية التي تتضمن



الشروط التعاقدية علي نحو معين، أو ما يعفي ذلك الطرف من العواقب القانونية لعدم قيامه بذلك.

#### **المادة ١٤**

##### **الخطأ في الخطابات الإلكترونية**

- ١- عندما يرتكب شخص طبعي خطأ في تخاطب إلكتروني مع نظام رسائل آلي تابع لطرف آخر ولا يوفر نظام الرسائل الآلي لذلك الشخص فرصة لتصحيح الخطأ، يحق لذلك الشخص، أو للطرف الذي يتصرف ذلك الشخص نيابة عنه، أن يسحب ذلك الجزء من الخطاب الإلكتروني الذي ارتكب فيه الخطاب الإلكتروني الذي ارتكب فيه الخطأ إذا:  
(أ) أبلغ الشخص، أو الطرف الذي يتصرف ذلك الشخص نيابة عنه، الطرف الآخر بالخطأ في أقرب وقت ممكن بعد علمه به، وذكر أنه ارتكب خطأ في الخطاب الإلكتروني.  
(ب) ولم يكن الشخص، أو الطرف الذي يتصرف ذلك الشخص نيابة عنه، قد استخدم ما قد يكون تسلمه من سلع أو خدمات من الطرف الآخر أو حصل منها علي أي منفعة أو قيمة مادية.
- ٢- ليس في هذه المادة ما يمس بانطباق أي قاعدة قانونية قد تحكم عواقب أي خطأ غير ما هو منصوص عليه في الفقرة ١.

#### **الفصل الرابع**

##### **أحكام ختامية**

#### **المادة ١٥**

##### **الوديعة**

يعين الأمين العام للأمم المتحدة بحكم هذه المادة وديعا لهذه الاتفاقية.

## المادة ١٦

### التوقيع أو التصديق أو القبول أو الإقرار

- ١- يفتح باب التوقيع على هذه الاتفاقية أمام جميع الدول في مقر الأمم المتحدة في نيويورك من ١٦ كانون الثاني/يناير ٢٠٠٦ إلى ١٦ كانون الثاني/يناير ٢٠٠٨.
- ٢- هذه الاتفاقية خاضعة للتصديق أو القبول أو الإقرار من جانب الدول الموقعة.
- ٣- يفتح باب الانضمام إلى هذه الاتفاقية أمام جميع الدول التي ليست دولا موقعة اعتبارا من تاريخ فتح باب التوقيع عليها.
- ٤- تودع صكوك التصديق والقبول والإقرار والانضمام لدى الأمين العام للأمم المتحدة.

## المادة ١٧

### مشاركة منظمات التكامل الاقتصادي الإقليمية

- ١- يجوز لأي منظمة تكامل اقتصادي إقليمية، مؤلفة من دول ذات سيادة ولها اختصاص في مسائل معينة تحكمها هذه الاتفاقية أن تقوم، بالمثل، بالتوقيع على هذه الاتفاقية أو التصديق عليها أو قبولها أو إقرارها أو الانضمام إليها. ويكون لمنظمة التكامل الاقتصادي الإقليمية في تلك الحالة ما للدولة المتعاقدة من حقوق وعليها ما على تلك الدول من التزامات، ما دام لتلك المنظمة اختصاص في مسائل تحكمها هذه الاتفاقية. وحيثما يكون عدد الدول المتعاقدة ذات أهمية في هذه الاتفاقية، لا تعد منظمة التكامل الاقتصادي الإقليمية دولة متعاقدة إضافة إلى الدول الأعضاء فيها التي هي دول متعاقدة.

٢- توجه منظمة التكامل الاقتصادي الإقليمية إلى الوديع، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام، إعلانا تحدد فيه المسائل التي تحكمها هذه الاتفاقية والتي أحيل الاختصاص بشأنها إلى تلك المنظمة من جانب الدول الأعضاء فيها.

وتسارع منظمة التكامل الاقتصادي الإقليمية بإبلاغ الوديع بأي تغييرات تطرأ على توزيع الاختصاصات المبينة في الإعلان الصادر بمقتضى هذه الفقرة، بما في ذلك ما يستجد من إحالات لتلك الاختصاصات.

٣- أي إشارة إلى "دولة متعاقدة" أو "دول متعاقدة" في هذه الاتفاقية تنطبق بالمثل على أي منظمة تكامل اقتصادي إقليمية حيثما اقتضى السياق ذلك.

٤- لا تكون لهذه الاتفاقية غلبة على أي قواعد متعارضة معها تصدر عن أي منظمة تكامل اقتصادي إقليمية وتسري على الأطراف التي تقع مقر أعمالها في دول أعضاء في تلك المنظمة، حسبما يبين في إعلان يصدر وفقا للمادة ٢١.

## المادة ١٨

### نفاذ الاتفاقية في الوحدات الإقليمية الداخلية

- ١- إذا كان للدولة المتعاقدة وحدتان إقليميتان أو أكثر تطبق فيها نظم قانونية مختلفة فيما يتعلق بالمسائل التي تتناولها هذه الاتفاقية، جاز لها أن تعلن، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام، أن هذه الاتفاقية تسري على جميع وحداتها الإقليمية أو على واحدة فقط أو أكثر من تلك الوحدات، وجاز لها أن تعدل إعلانها في أي وقت بإصدار إعلان آخر.
- ٢- تبلغ هذه الإعلانات إلى الوديع وتذكر فيها صراحة الوحدات الإقليمية التي تسري عليها الاتفاقية.

٣- إذا كانت هذه الاتفاقية، بحكم إعلان صادر بمقتضى هذه المادة، تسري علي واحدة أو أكثر من الوحدات الإقليمية للدولة المتعاقدة ولكن ليس عليها جميعا، وكان مقر عمل الطرف واقعا في تلك الدولة، لا يعتبر مقر العمل هذا، لأغراض هذه الاتفاقية، واقعا في دولة متعاقدة ما لم يكن واقعا في وحدة إقليمية تسري عليها الاتفاقية.

٤- إذا لم تصدر الدولة المتعاقدة إعلانا بمقتضى الفقرة ١ من هذه المادة، كانت الاتفاقية سارية علي جميع الوحدات الإقليمية لتلك الدولة.

## **المادة ١٩**

### **الإعلانات المتعلقة بنطاق الانطباق**

١- يجوز لأي دولة متعاقدة أن تعلن، وفقا للمادة ٢١، أنها لن تطبق هذه الاتفاقية إلا:

(أ) عندما تكون الدول المشار إليها في الفقرة ١ من المادة ١ دولا متعاقدة في هذه الاتفاقية، أو

(ب) عندما تكون الأطراف قد اتفقت علي انطباقها.

٢- يجوز لأي دولة متعاقدة أن تستبعد من نطاق انطباق هذه الاتفاقية المسائل التي تذكرها تحديدا في إعلان تصدره وفقا للمادة ٢١.

## **المادة ٢٠**

### **الخطابات المتبادلة بمقتضى الاتفاقيات الدولية**

- تنطبق أحكام هذه الاتفاقية علي استخدام الخطابات الإلكترونية في سياق تكون أو تنفيذ عقد تسري عليه أي من الاتفاقيات الدولية التالية، التي تكون الدولة المتعاقدة في هذه الاتفاقية، أو قد تصبح، دولة متعاقدة فيها:

اتفاقية الاعتراف بقرارات التحكيم الأجنبية وإنفاذها (نيويورك، ١٠ حزيران/يونيه ١٩٥٠).

اتفاقية فترة التقادم في البيع الدولي للبضائع (نيويورك، ١٤ حزيران/يونيه ١٩٧٤) البروتوكول الملحق بها (فيينا، ١١ نيسان/إبريل ١٩٨٠).  
اتفاقية الأمم المتحدة المتعلقة بعقود البيع الدولي للبضائع (فيينا، ١١ نيسان/إبريل ١٩٨٠).

اتفاقية الأمم المتحدة المتعلقة بمسؤولية متعهدي خدمات المحطات النهائية للنقل في التجارة الدولية (فيينا، ١٩ نيسان/إبريل ١٩٩١).

اتفاقية الأمم المتحدة المتعلقة بالكفالات المستقلة وخطابات الاعتماد الضامنة (نيويورك، ١١ كانون الأول/ديسمبر ١٩٩٥).

اتفاقية الأمم المتحدة لإحالة المستحقات في التجارة الدولية (نيويورك، ١٢ كانون الأول/ديسمبر ٢٠٠١).

- تنطبق أحكام هذه الاتفاقية كذلك علي استخدام الخطابات الإلكترونية في سياق تكوين أو تنفيذ عقد يسري عليه أي من الاتفاقيات أو المعاهدات أو الاتفاقات الدولية الأخرى غير المذكورة تحديدا في الفقرة ١ من هذه المادة والتي تكون الدولة المتعاقدة في هذه الاتفاقية، أو قد تصبح، دولة متعاقدة فيها، ما لم، تكن تلك الدولة قد أعلنت، وفقا للمادة ٢١، أنها لن تكون ملزمة بهذه الفقرة.

- يجوز لأي دولة تصدر إعلانا عملا بالفقرة ٢ من هذه المادة أن تعلن أيضا بها ستطبق أحكام هذه الاتفاقية، علي الرغم من ذلك، علي استخدام الخطابات الإلكترونية في سياق تكوين أو تنفيذ أي عقد يسري عليه أي من الاتفاقيات أو المعاهدات أو الاتفاقيات الدولية المحددة التي تكون تلك الدولة أو قد تصبح دولة متعاقدة فيها.

٤- يجوز لأي دولة أن تعلن أنها لن تطبق أحكام هذه الاتفاقية علي استخدام الخطابات الإلكترونية في سياق تكوين أو تنفيذ عقد يسري عليه أي من الاتفاقيات أو المعاهدات أو الاتفاقيات الدولية المذكورة تحديدا في الإعلان الصادر عن تلك الدولة والتي تكون تلك الدولة، أو قد تصبح، دولة متعاقدة فيها، بما في ذلك أي من الاتفاقيات المشار إليها في الفقرة ١ من هذه المادة، حتى وإن لم تستبعد تلك الدولة تطبيق الفقرة ٢ من هذه المادة بإعلان تصدره وفقا للمادة ٢١.

## المادة ٢١

### إجراءات إصدار الإعلانات وسريان مفعولها

١- يجوز إصدار الإعلانات بمقتضى الفقرة ٤ من المادة ١٧ والفقرتين ١ و ٢ من المادة ١٩ والفقرات ٢ و ٣ و ٤ من المادة ٢٠ في أي وقت. أما الإعلانات التي تصدر وقت التوقيع علي الاتفاقية فهي تخضع للتأكيد عند التصديق أو القبول أو الإقرار.

٢- تكون الإعلانات وتأكيداتها مكتوبة وتبلغ إلي الوديع رسميا.

٣- يسري مفعول الإعلان في آن واحد مع بدء نفاذ هذه الاتفاقية فيما يخص الدولة المعنية أما الإعلان الذي يبلغ به الوديع رسميا بعد بدء نفاذ الاتفاقية فيسري مفعوله في اليوم الأول من الشهر الذي يعقب انقضاء ستة أشهر علي تاريخ تلقي الوديع إشعارا به.

٤- يجوز لأي دولة تصدر إعلانا بمقتضى هذه الاتفاقية أن تعدله أو تسحبه في أي وقت بإشعار رسمي مكتوب يوجه إلي الوديع. ويسري مفعول التعديل أو السحب في اليوم الأول من الشهر الذي يعقب انقضاء ستة أشهر علي تاريخ تلقي الوديع ذلك الإشعار.

## **المادة ٢٢**

### **التحفظات**

لا يجوز تقديم تحفظات في إطار هذه الاتفاقية.

## **المادة ٢٣**

### **بدء النفاذ**

١- يبدأ نفاذ هذه الاتفاقية في اليوم الأول من الشهر الذي يعقب انقضاء ستة أشهر علي تاريخ إيداع الصك الثالث من صكوك التصديق أو القبول أو الإقرار أو الانضمام.

٢- 'عندما تصدق أي دولة علي هذه الاتفاقية أو تقبلها أو تقرها أو تنضم إليها بعد إيداع الصك الثالث من صكوك التصديق أو القبول أو الإقرار أو الانضمام، يبدأ نفاذ هذه الاتفاقية فيما يخص تلك الدولة في اليوم الأول من الشهر الذي يعقب انقضاء ستة أشهر علي تاريخ إيداع صك تصديق أو قبولها أو إقرارها أو انضمامها.

## **المادة ٢٤**

### **وقت الانطباق**

لا تنطبق هذه الاتفاقية ولا أي إعلان إلا علي الخطابات الإلكترونية التي توجهه بعد التاريخ الذي يبدأ فيه نفاذ الاتفاقية أو يسري فيه مفعول الإعلان فيما يخص كل دولة متعاقدة.

## المادة ٢٥

### الانسحاب

- ١- يجوز للدولة المتعاقدة أن تعلم انسحابها من هذه الاتفاقية بإشعار رسمي يوجه إلى الوديع كتابة.
- ٢- يسري مفعول الانسحاب في اليوم الأول من الشهر الذي يعقب انقضاء اثني عشر شهرا علي تلقي الوديع إشعارا به. وعندما تحدد في الإشعار فترة أطول من تلك فيسري مفعول الانسحاب عند انقضاء تلك الفترة الأطول بعد تلقي الوديع ذلك الإشعار.
- حررت في نيويورك، في هذا اليوم (.....) من شهر (.....) من عام ٢٠٠٥، في أصل واحد تتساوي في الحجية نصوصه الإسبانية والإنكليزية والروسية والصينية والعربية والفرنسية.
- وإثباتاً لما تقدم، قام المفوضون الموقعون أدناه، المخولون حسب الأصول من قبل حكوماتهم، بالتوقيع علي هذه الاتفاقية.



## فهرس

الموضوع	الصفحة
مقدمة .....	٣
باب تمهيدى	٧
فى التوقيع الإلكترونى	
- آداب السلوك الأساسية على إنترنت.....	٩
- فيروسات الكمبيوتر.....	١٤
- برنامج مكافحة الفيروسات.....	٢١
- طرق للمساعدة على تجنب الأطفال قرصنة الملفات عبر إنترنت	٢٧
- أنواع التخزين الخارجى.....	٣٧
- عولمة الأسواق.....	٤٧
- دور التطورات المعاصرة فى ظهور الجرائم الإلكترونية.....	٤٩
- تصنيف وأشكال الجرائم الإلكترونية.....	٥٠
أولاً: تصنيف الجرائم حسب مواطن الاختراق.....	٥٠
ثانياً: تصنيف الجرائم حسب مساسها بالأشخاص والأموال.....	٥١
- الملكية الفكرية للمصنفات الرقمية.....	٥٢
- المخاطر الأمنية للإنترنت .....	٦٠
الفصل الأول	٦٥
فيروسات الحاسبات	
أنواعها وأشكالها وكيفية مواجهتها	
- أمور تتعلق بالإنترنت.....	٦٧
- مخاطر الإنترنت المحتملة.....	٦٧
- جواسيس الإنترنت .....	٧٥
- بعض نماذج الفيروسات.....	٨٠
- جرائم الاحترافات عبر الإنترنت.....	٨٢

- ١٠٧ - الجرائم الإلكترونية.....
- ١٠٨ - الحماية من الجرائم الإلكترونية.....
- ١٠٩ - سيناريوهات حروب المعلومات.....
- ١١١ - سبل الحماية.....
- ١١٣ - محارب جرائم الإنترنت.....
- ١٢٤ - جرائم التجسس والإرهاب الإلكتروني عبر الإنترنت.....
- ١٣١ - آليات الحماية.....

- ١٨٦ - السنطاق القانوني لحماية برامج الكمبيوتر وقواعد البيانات في البيئة العربية.....
- ١٨٩ - إشكالات حماية البرمجيات وقواعد البيانات.....
- ٢٠٠ - حماية البرمجيات بين تطبيق القانون وأثره على الدول النامية....
- ٢١٤ - خصوصية جرائم الكمبيوتر والإنترنت.....
- ٢٢٥ - إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات.....
- ٢٣٥ - التحقيق في جرائم الحاسوب.....

## الاتفاقيات الدولية على المستوى الدولي

## وعلى المستوى الإقليمي للدول العربية

- أولاً: اتفاقية برن لحماية المصنفات الأدبية والفنية..... ٢٤٥
- ثانياً: مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبات الإلكترونية..... ٣٠٥
- ثالثاً: مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر..... ٣١١
- رابعاً: قرار بشأن الجرائم ذات الصلة بالكمبيوتر..... ٣١٧
- خامساً: الإعلان الخامس باستخدام التقدم العلمي والتكنولوجي لصالح السلك وخير البشرية..... ٢٣٢
- سادساً: القمة العالمية لمجتمع المعلومات..... ٣٣٧
- سابعاً: قرارات القمة العربية بشأن تكنولوجيا المعلومات والاتصالات لمواجهة الثورة العلمية والتقنية الراهنة..... ٤١٧
- ثامناً: وثيقة إعلان الاستراتيجية العربية لمجتمع الاتصالات وتقنية المعلومات..... ٤٢٥
- تاسعاً:
- ١- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية ٢٠٠١..... ٤٥٢
- ٢- دليل اشتراخ قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام ٢٠٠١..... ٤٦٠
- ٣- اتفاقية الأمم المتحدة المتعلقة باستخدام خطابات الإلكترونية.... ٥٦٧

